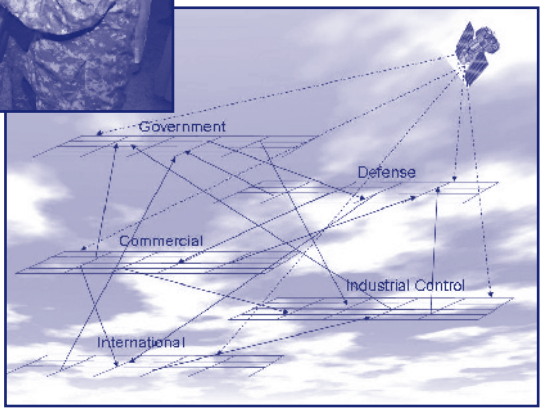

INFORMATION AS POWER

AN ANTHOLOGY OF SELECTED UNITED STATES ARMY WAR COLLEGE STUDENT PAPERS

VOLUME 6

Edited by
Jeffrey L. Groh, Benjamin C. Leitzel,
Dennis M. Murphy, and Mark A. Van Dyke

U.S. ARMY WAR COLLEGE

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
MAY 2012		**00-00-2012 to 00-00-2012**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Information as Power: An Anthology of Selected United States Army War College Student Papers. Volume 6	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **U.S. Army War College,Center for Strategic Leadership and Development ,650 Wright Avenue ,Carlisle,PA,17013-5049**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**197**	

U.S. ARMY WAR COLLEGE

INFORMATION AS POWER

VOLUME 6

AN ANTHOLOGY OF SELECTED UNITED STATES ARMY WAR COLLEGE STUDENT PAPERS

Information as Power is a refereed anthology of United States Army War College (USAWC) student papers related to information as an element of national power. It provides a medium for the articulation of ideas promulgated by independent student research in order to facilitate understanding of the information element of power and to better address related national security issues. The anthology serves as a vehicle for recognizing the analyses of Army War College students and provides a resource for USAWC graduates, senior military officers, and interagency national security practitioners concerned with the information element of national power.

Special thanks to Benjamin C. Leitzel who authored the section introductions and for his significant editorial and administrative support, to Ritchie Dion and Elizabeth Heffner for their meticulous layout editing, and to Jennifer Nevil for the cover design.

Information as Power


U.S. ARMY WAR COLLEGE
Prudens
Futuri
Carlisle Barracks, PA

INFORMATION AS POWER

An Anthology of Selected United States Army War College Student Papers

Volume Six

Editors:

Jeffrey L. Groh,
Benjamin C. Leitzel, Dennis M. Murphy,
and Mark A. Van Dyke

Information as Power

An Anthology of Selected United States Army War College Student Papers

Volume Six

Executive Agent for the Anthology:
United States Army War College

Published May 2012.

This publication is available on line at the following:

http://www.carlisle.army.mil/dime or,

http://www.csl.army.mil/InfoAsPower.aspx

Cover photograph by Staff Sgt. DeNoris A. Mickle, USAF.
Used by permission.

U.S. ARMY WAR COLLEGE
CARLISLE BARRACKS, PENNSYLVANIA 17013

Contents


U.S. ARMY WAR COLLEGE
Prudens
Futuri
Carlisle Barracks, PA

Preface

The U.S. Army War College (USAWC) is pleased to present this anthology of selected student work from Academic Year 2011 representing examples of well-written and in-depth analyses on the vital subject of Information as Power. This is the sixth volume of an effort that began in 2006. The anthology is an important component of an effort to coordinate and recommend the design, development and integration of content and courses related to the information element of power into the curriculum to prepare our students for senior leadership positions.

Interestingly, one needs to go back to the Reagan administration to find the most succinct and pointed mention of information as an element of power in formal government documents.[1] Subsequent national security documents, to include the 2010 National Framework for Strategic Communication and the current National Security Strategy, allude to different aspects of information but without a holistic, overarching strategy or definition. Still, it is generally accepted in the United States government today that information is an element of national power along with diplomatic, military and economic power… and that information is woven through the other elements since their activities will have an informational impact. Given this dearth of official documentation, Drs. Dan Kuehl and Bob Nielson proffered the following definition of the information element: "Use of information content and technology as strategic instruments to shape fundamental political, economic, military and cultural forces on a long-term basis to affect the global behavior of governments, supra-governmental organizations, and societies to support national security."[2] Information as power is wielded in a complex environment consisting of the physical, informational, and cognitive dimensions (alternatively referred to as "connectivity, content and cognition").

The current information environment has leveled the playing field for not only nation states, but non-state actors, multinational corporations and even individuals to cognitively affect strategic outcomes with minimal information infrastructure and little capital expenditure.

Anyone with a camera cell phone or personal digital device with Internet capability understands this. Adversary use of information as an asymmetric strategic means has been extremely effective in Iraq and Afghanistan. On the other hand, the U.S. government and its military exploit the capabilities of cyberspace to communicate effectively, conduct daily business and plan and execute military operations. This capability, however, becomes a vulnerability of dependence that can be targeted by rogue individuals, criminals and adversary nation states. Clearly, managing the message while protecting the necessary technological means represent critical opportunities and challenges requiring risk analysis and mitigation.

U.S. strategic thought on these issues has advanced over the past six years as has the research and analysis of our students about these information-related topics. "Information as Power" is reflective of that intellectual evolution. We've moved from a discussion of what defines strategic communication in Volume 1 to the important but difficult process of measuring strategic communication effectiveness in this latest edition. We've shifted from a focus on network centric operations to future-focused strategic and operational analyses of cyberspace. As such, the anthology serves not only to showcase the efforts of the College but to inform the broader body of knowledge as the Nation advances its efforts to act proactively within this environment and to counter current and potentially future adversaries who so effectively exploit it.

Professor Dennis M. Murphy
Director, Information in Warfare Group
United States Army War College
Carlisle, Pennsylvania

Section One

Information Effects in the Cyberspace Domain


U.S. ARMY WAR COLLEGE
Prudens
Futuri
Carlisle Barracks, PA

Introduction

Cyberspace provides us with enormous opportunities; however as our reliance on this interdependent information network increases we must be aware of its significant vulnerabilities. The United States' energy, banking, transportation, and communications systems rely on cyberspace. The Department of Defense is dependent on cyberspace to function as it "operates over 15,000 networks and seven million computing devices across hundreds of installations in dozens of countries around the globe."[1] Senior leaders must enhance their understanding of the cyberspace domain to take advantage of the opportunities, reduce vulnerabilities and operate more effectively. This section highlights three excellent student papers that examine challenges and opportunities in various aspects of cyberspace theory and practice.

The first paper is an award winning essay, "Securing Cyberspace: Approaches to Developing an Effective Cyber-Security Strategy," by Lieutenant Colonel Douglas Smith. In this paper, he asserts that protection of cyberspace is a national security priority for which the United States must develop a comprehensive cyber strategy to deter, defend against, and respond to cyber attacks. After examining the characteristics and implications of hostile cyber attacks, he recommends three concepts that should be included in the cyber strategy.

In his award winning essay, "A Strategic Approach to Network Defense: Framing the Cloud," Colonel Timothy Buennemeyer examines current cyber attack trends in the computer networking environment and proposes an enhanced framework for system defense that is applicable to both corporate and government networks. He shows that computer defensive measures are not uniformly implemented and as the U.S. government migrates its vast network of computer systems to an enterprise-focused architecture, it must implement this enhanced security framework. Colonel Buennemeyer recommends basing this framework on accepted network defensive principles, with the goal to reduce risks associated with emerging virtualization capabilities and scalability of cloud computing.

Colonel Bryan DeCoster writes a persuasive essay on the legal implications of cyberspace operations titled, "Crime or War: Cyberspace Law and its Implications for Intelligence." He posits that international law must be refined to distinguish between crimes and potential acts of war for activities in cyberspace. Colonel DeCoster then analyzes cyberspace threats in terms of existing law to determine which threats and their relevant cyberspace activities are matters for law enforcement as opposed to potential acts of war to be pursued by the Department of Defense. Finally, he proposes several imperatives for the intelligence community that addresses the international legal status and constraints on use of force and armed attacks that can be applied to the cyberspace environment.

These well written and insightful papers reflect a depth of research and thought concerning the cyberspace domain. They lay the groundwork for the development of new and innovative ideas to meet the information requirements emerging in future military, government, and commercial ventures.

Securing Cyberspace: Approaches to Developing an Effective Cybersecurity Strategy

Lieutenant Colonel Douglas S. Smith
United States Army Reserve

Cyberspace has become part of the fabric of the modern world. Internet usage is growing exponentially, from one million internet users in 1992, to 1.2 billion users in 2007, to over two billion in 2010.[1] Society increasingly relies on cyberspace tools to regulate infrastructure critical to daily life, such as electric power grids, global finance, banking, transportation, healthcare and telecommunications. The nation's military depends on networks for command and control, communications, intelligence, logistics and weapons systems. Although few would deny the benefits that cyberspace has brought to nearly every facet of life, reliance on free access to cyberspace makes society vulnerable to disruptions caused by malicious attackers, cyber-criminals or even teenage hackers.

Protecting cyberspace is a national security priority. President Obama's National Security Strategy (NSS) acknowledges that threats to cybersecurity "represent one of the most serious national security, public safety, and economic challenges we face as a nation."[2] The Quadrennial Defense Review (QDR) Report states that in the 21st century, "modern armed forces simply cannot conduct high-tempo, effective operations without resilient, reliable information and communication networks and assured access to cyberspace."[3] These statements support the assertion that the United States has a vital national interest in cyberspace, with free and unencumbered access for innovation, global commerce and communications, and with robust security to protect the digital infrastructure that powers critical national functions. The NSS articulates the strategic objective that supports this interest: "deter, prevent, detect, defend against, and quickly recover from cyber intrusions and attacks."[4] The United States needs a comprehensive cyber strategy to achieve this objective (ends) that includes conceptual approaches (ways) in three broad areas: (1) U.S. government and

military policies for cyberspace defense, (2) international influence in cyberspace, and (3) deterrence of cyber attacks.

The Nature of Conflict in Cyberspace

Development of a comprehensive cybersecurity strategy requires an understanding of cyberspace and the nature of conflict within it. This section discusses definitions for cyberspace, cyber power, cyber attack and cyber exploitation and recent examples of how cyber-conflict has embroiled the physical world.

The term *cyberspace*, coined in 1984,[5] has been described in numerous contexts within science fiction, academia, government, and the military. Many sources describe cyberspace as a global operational domain and compare its qualities to the physical domains: land, sea, air and space. Human use of each domain followed from technological innovation. The space domain, for example, was unimportant to society before development of rockets and satellites. Today's communications would be impossible without operational capabilities in space. Advances in electronics and computers created cyberspace, the first man-made domain, and opened it to human exploration and exploitation.

The Joint Chiefs of Staff define cyberspace as a global domain within the information environment, encompassing the "interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems and embedded processors and controllers."[6] The Joint Chiefs of Staff describe cyberspace as "the use of electronics and the electromagnetic spectrum to create, store, modify, exchange and exploit information."[7] The implication of this definition is that cyberspace represents not just the technical aspects of the medium, such as networks and computers, but also the information itself and the human element that shapes and interprets the information.

Protecting strategic interests in cyberspace requires effective application of cyber power. Daniel Kuehl, Director of the Information Strategies Concentration Program at the National War College, defines cyber power as "the ability to use cyberspace to create advantages and influence events in all the operational environments and across the instruments

of power."[8] This definition is reminiscent of Mahan's concept of sea-power: "a nation's ability to enforce its will upon the sea."[9] The nation wielding sea-power has capabilities to guarantee free access across the oceans for its own purposes and interests and to prevent adversaries from impeding the same. Similarly, the nation wielding cyber power has capabilities to patrol cyberspace and take actions to secure its own interests within cyberspace and prevent adversaries from impeding the same. Unlike the physical domains, however, cyberspace creates effects in all five domains. Consequently, cyber power is applicable to all operational domains and all elements of national power.

Conflict in cyberspace can occur in one of two forms: cyber attack or cyber exploitation. Although there is no consensus of what constitutes a cyber attack, all are comprised of a deliberate action taken to "alter, disrupt, deceive, degrade, or destroy" systems or networks in cyberspace.[10] The scale of attacks can vary widely, ranging from the inconvenience of a user locked out of a network to complete shutdown of critical control systems.

Cyber attacks share four important characteristics.[11] First, the indirect effects of the attack are often more consequential than the direct effects. An attack against the controls of a power grid, for example, could cause blackouts, similar to what might occur during natural disasters. The indirect effects might outweigh the direct effects, such as interruptions to commerce, creation of opportunities for crime, public outcry and reduced investment. For example, cyber attacks to the power grid caused several wide-spread blackouts in Brazil and Paraguay in 2005, 2007 and 2009. Although the most recent outage only lasted for two hours, the incident created the perception that the infrastructure in South America is vulnerable. International perceptions disproportionately bruised Brazil's reputation, undermining confidence in their ability to host the 2016 Olympic Games and soccer's 2014 World Cup.[12]

Second, the technology to launch a cyber attack is relatively inexpensive and readily available. As a result, non-state actors have adopted cyber attacks as a weapon of choice. Small groups can develop sophisticated capabilities to conduct cyber attacks against large, well resourced entities for economic or political purposes. For example, a three-week cyber-attack raged in Estonia in 2007. The dispute erupted when

Russians protested the Government of Estonia's announcement that it would remove a Soviet war memorial, the "Bronze Soldier of Tallinn."[13] Russian hackers attacked numerous government agencies, banks and news organizations, intermittently shutting down networks and disrupting life in Estonia.[14] Russian individuals appeared to perpetrate the attacks inside and outside of Russia, without proven support from the Russian Federation. The conflict illustrates what cyber-war may look like in the future: small, technically advanced groups attack the digital infrastructure of nations in pursuit of a political objective.

Third, cyber attacks may be highly asymmetric. A common weapon in cyberspace is the *botnet*, a large number of infected computers remotely controlled by a master computer. A botnet grows when a virus infects ordinary computers across the Internet, creating virtual links between them without users' knowledge. The perpetrator can remotely activate an army of computers against specific targets, to overwhelm networks, block or disrupt access to systems or infect other computers and networks.[15] One example is the Mariposa botnet, made up of 13 million infected computers, created and controlled by just a few individuals.[16] After infecting an unsuspecting computer, the program monitored activity for passwords and banking and credit card information. The Internet's openness allows a single user to amplify influence.

Fourth, perpetrators can conceal their identities with relative ease if they seek anonymity. For example, the Conficker Worm is a propagating and mutating virus that has infected an estimated 10 million computers, creating the framework for a powerful botnet ready to launch an attack at its creator's signal. Despite unprecedented international collaboration and even a bounty offer standing since 2009, the identity and motives of the worm's creators remain a mystery. A botnet this large could theoretically "paralyze the infrastructure of a major Western nation."[17]

Cyber exploitation involves the use of offensive actions within cyberspace but unlike cyber attacks normally does not seek to disrupt the normal functioning of the targeted network or systems. The objective of cyber exploitation is usually to obtain information for illegitimate purposes, including espionage, theft of confidential information such as credit card or personal information or other criminal reasons.[18] For example, China has directed cyber-espionage efforts against the U.S.

Department of Defense since 2002, with successful theft of 10 to 20 terabytes of data from military networks.[19]

As the world becomes more interconnected, cyber power increasingly is "exerting itself as a key lever in the development and execution of national policy."[20] An effective cyber strategy will benefit numerous national efforts, including counter-terrorism, economic development, fighting crime, diplomatic engagement and intelligence gathering.

U.S. Government and Military Policies for Cyberspace Defense

Governance of cyberspace is an elusive concept. The term *governance* is misleading because governments currently exercise little control over internet policy or protocols. Instead, an evolving collection of private and commercial organizations determine policies and protocols by consensus to keep the Internet functioning smoothly. One such organization is the Internet Corporation for Assigned Names and Numbers (ICANN), a private, non-profit corporation responsible for assigning domain names, the unique identifier that gives information a place to exist on the Internet ("www.microsoft.com," for example, is the assigned domain name for the Microsoft Corporation). ICANN has a government advisory committee open to any national government, but members may only advise ICANN's Board of Directors and do not have voting rights on board policies.[21] Other forums are responsible for other cyberspace functions, such as communications standards and core internet functions.[22] These organizations have evolved in an ad hoc manner driven mainly by the need to resolve technical issues. But where once technical problem-solving was an academic notion necessary for establishing cyber infrastructure, today the need to fight cyber exploitation and cyber attack lends a heightened urgency for proper conduct within cyberspace. Given the present state of governance, public policy-makers should seek to develop greater influence on certain aspects of cyberspace, rather than adopt true governance.[23] Government initiatives should include three approaches to cybersecurity: (1) a differentiated approach to security policy, (2) a centralized approach to protect military cyber-assets under U.S. Cyber Command and (3) a holistic interagency approach, as begun with the Comprehensive National Cybersecurity Initiative.

First, the U.S. government should develop a differentiated approach to cybersecurity, with the intent of prioritizing the wide variety of cyber attacks and cyber exploitations and appropriately focusing counter-measures. The first step is to prioritize cyber attacks and cyber exploitations with regard to their possible consequences. On one end of the spectrum are the nuisance hackers who probe networks thousands of times each day. On the other end is the sophisticated cyber attack that causes damages commensurate with an act of war. This approach should classify cyber capabilities as *indispensable*, *key* or *other*. *Indispensable* cyber would include critical military capabilities or civil security capabilities that the country could not be without even for a short time.[24] *Key* cyber also include critical infrastructure where temporary workarounds are possible. This may include electric grids, financial networks, transportation systems and certain military or intelligence capabilities whose exploitation would damage national security. The vast bulk of cyber capabilities remaining would fall into the *other* category. Next, the federal government should tailor security measures for each category. For *indispensable* cyber, the federal government should provide security directly. Activities should include actively monitoring for attacks, providing cyber defenses and redundant systems. For *key* cyber, the U.S. government should develop policies and regulations that require minimum levels of protection for cyber capabilities that reside with private or state control and provide adequate resources for law enforcement and security cooperation with entities that have responsibility for key cyber capabilities. For *other* cyber, the government could encourage improved cybersecurity through education, incentives or voluntary participation in government security programs.

Second, U.S. Cyber Command (CYBERCOM) has assumed responsibility for protection of critical government and military cyber assets. It achieved full operational capability on November 3, 2010, as a four-star, sub-unified command under U.S. Strategic Command.[25] CYBERCOM's three-prong mission is to: (1) operate and defend DOD networks, (2) prepare to conduct full-spectrum military cyberspace operations, and (3) defend U.S. freedom of action in cyberspace.[26] CYBERCOM executes its first mission with a layered defense of the Global Information Grid (GIG). The outer most layer of protection

is "ordinary hygiene," which includes keeping malware protection, firewall, and anti-virus software up to date on 15,000 networks within the .mil domain and seven million computers.[27] Diligent hygiene blocks about half of attempted intrusions. The next line of defense is "perimeter security," which monitors traffic in and out of DOD networks.[28] CYBERCOM has limited the number of access ports to DOD systems from the Internet, creating cyber choke points where it can more effectively marshal defenses. Perimeter security blocks an additional 30-40% of attempted intrusions. Finally, CYBERCOM conducts dynamic defenses to block the last 10% of attempted intrusions. Dynamic defense systems act in real-time as "part sensor, part sentry, part sharpshooter."[29] They continuously monitor traffic, automatically identify intruders and block access. In contrast, static defenses, such as hygiene activities, wait and react to intruders after they have penetrated the network. The National Security Agency (NSA) leads the initiative to develop dynamic defenses. In addition to technical capabilities, NSA will incorporate foreign intelligence to anticipate threats. Effective unity of effort is possible with U.S. Army General Keith Alexander acting as both CYBERCOM's Commander and NSA's Director. A challenge remaining for CYBERCOM will be to develop mechanisms to extend cyber protection to key cyber capabilities that reside outside of DOD-controlled networks. Although General Alexander cites the importance of the principle, he admits that older cyber-systems powering electric grids, banking and transportation systems are inherently more difficult to defend.[30] The military also depends on commercial and unclassified networks for much of its communications and records-keeping. Industry should apply lessons learned from CYBERCOM's efforts to protect the GIG to cybersecurity for critical civilian sectors.

Third, the U.S. should pursue a holistic interagency approach to cybersecurity. The Comprehensive National Cybersecurity Initiative (CNCI) is an excellent template for success. The Bush administration launched this initiative in January, 2008, in response to a series of cyber attacks on multiple federal agency networks. A major goal of this initiative was to unify agencies' approach to cybersecurity. Under the Obama administration, it has evolved into a broader cybersecurity strategy. The CNCI defines 12 initiatives to facilitate collaboration

among federal and state governments and the private sector that ensure an organized and unified response to cyber attacks.[31] For example, the Trusted Internet Connections program, an initiative led by the Office of Management and Budget (OMB) and the Department of Homeland Security (DHS), consolidates access ports to Federal Government systems, much as CYBERCOM has done for military systems.[32] Agencies can more easily monitor and defend fewer access ports. Another initiative involves deployment of an intrusion detection and prevention system for civilian government networks DHS developed and deployed the EINSTEIN 2 program to automatically detect unauthorized or malicious network traffic across U.S. Government networks and send real-time alerts to the U.S. Computer Emergency Readiness Team (US-CERT), the operational arm of the National Cyber Security Division within DHS charged with coordinating the federal response to cyber attacks.[33] DHS is also working to pilot technology developed by the NSA as EINSTEIN 3, to conduct "real-time full packet inspection and threat-based decision-making" with the ability to automatically respond to cyber threats before harming the network.[34] Another initiative calls for connecting strategic cyber operations centers to enhance situational awareness across agency networks and systems and foster interagency collaboration and coordination. The intent is for the National Cybersecurity Center (NCSC) within the DHS to connect six existing cyber centers within DHS, DOD, FBI, NSA and Office of Director of National Intelligence (ODNI) to share information with each other through relationships and liaison officers.[35] Together, the centers create common situational awareness among key cyber functions, including cyber-intelligence, counter-intelligence, cyber-crime investigation and law enforcement, civil and defense collaboration and intrusion detection and response.

These initiatives show remarkable progress on creating a holistic, interagency approach to protecting government systems against cyber attack. Like other interagency efforts competing agency interests will challenge the CNCI's control of significant resources targeted for cybersecurity, and by public debate about the proper role for federal regulations. In 2009, for example, the Director of the NCSC resigned in protest of the increasingly prominent role played by the NSA in cyber efforts. The Director argued in favor of checks and balances by

separating security powers among government agencies, and cited "threats to democratic processes…if all top-level government network security and monitoring are handled by any one organization."[36] This initiative continues amid public debate on the appropriate role that government oversight and control should play in balancing protection against cyber attack with free and open access to cyberspace.[37]

International Influence in Cyberspace

Private sector entities and individuals have few effective and legal alternatives to respond to a cyber attack or cyber exploitation. The first line of defense is to strengthen their passive defensive measures, including dropping services that are targeted or closing firewall ports to deny access to key systems. These measures cannot completely protect systems against increasingly sophisticated attackers and deny the victim the benefits of key services or connections.[38] The second option is to report the cyber attack or cyber exploitation to the authorities for prosecution. Questions of global jurisdiction complicate prompt investigation and prosecution. If a U.S. company is a target of a cyber attack in its Japanese offices by the Russian mob through a server located in Brazil, where does the jurisdictional authority lie for prosecuting the attack?[39] To improve effectiveness of cyber efforts in a globally connected world, the United States should exercise diplomatic means to seek common ground among countries and intergovernmental organizations for fighting against cyber attacks and cyber exploitation and to influence international partners to collaborate on core areas of cybersecurity.

Effective policy-making to encourage international cooperation requires an understanding of how different cultures give rise to different attitudes and norms about fighting cyber attacks. The United States, for example, prefers to engage international law enforcement to investigate and catch cyber criminals.[40] International cooperation could resolve jurisdictional issues when perpetrators conduct cyber attacks across state lines. INTERPOL conducts a similar function for fighting international crime by providing liaison between law enforcement authorities among its 188 member countries.[41] It provides a model for international cooperation that could apply to cyber-crime.

In contrast, Russia argues that the U.S. approach would lead to interference in its internal affairs. Russia jealously protects non-interference, an "immutable principle of international law," as a pillar of her sovereignty.[42] Russia tends to be wary of American motives, which it claims have political and ideological goals aimed at undermining Russian independence and its sphere of influence in Eastern Europe. Russia's actions and policies also conveniently protect its own population of patriotic hackers, an educated and empowered volunteer militia within cyberspace. These were the foot-soldiers during the cyber-conflict that occurred during the Georgia-Russia conflict of 2008.[43] One day after Russia invaded Georgia, the StopGeorgia.ru forum began conducting a series of denial-of-service attacks against Georgian government websites that disabled several key websites during the invasion. Sophisticated hackers ran the StopGeorgia.ru forum who published lists of vetted targets that patriotic Russian hackers attacked. Although the Russian Government distanced itself from the hacker activity, it clearly enjoyed the benefits and tacitly supported the community. International law enforcement cooperation, as espoused by the United States, could target these non-state hackers.

China has a third view. Chinese authorities closely monitor Chinese networks and take aggressive steps to filter or block what the government considers "politically troublesome content," such as references to democracy, civil liberties, Chinese political dissidents and other concepts contrary to Red ideology.[44] The alleged intent of China's internet crack-down is to protect civil order. Supporters of free speech decry these practices as censorship and a pretext for the government to tighten its control over daily life and solidify its power. The three approaches illustrate the divergent attitudes toward cyberspace and underscore the complexity in attempting to influence international norms and behavior.

With an understanding of cultural differences about cyberspace, American diplomatic efforts should seek common ground among countries to cooperate in promoting cybersecurity and combating cyber attacks. The United States should advocate that cyberspace is a global commons whose usefulness is contingent upon its security. The United States needs to apply diplomatic pressure to influence countries

to adopt collaborative practices in finding and blocking cyber attacks. One such collective approach is the Council of Europe's Convention on Cybercrime. Thirty countries have ratified the convention, including the United States, and 17 others are signatories. The convention requires that signatories enact stringent laws against cyber-crime and take steps to investigate and prosecute violators. The convention also directs participating countries to cooperate with one another in such matters as reciprocal law, extradition and mutual assistance.[45] A weakness of the convention is that while it mandates public action, it establishes few means to verify compliance. The convention is currently open for signatures but differences in cultural attitudes discussed above present barriers to wider acceptance. The United States should use diplomatic pressure to encourage wider acceptance of the Convention's principles.

The international community should develop the concept of a sanctuary state to bring pressure to bear on states who fail to discharge their duty to prevent cyber attacks. The 9/11 attacks on the World Trade Centers and the Pentagon introduced a new paradigm for fighting terrorism. The resulting doctrine prescribed that the United States would not only fight terrorists but also the regimes that harbored and sheltered them. Similarly, a state that fails to prosecute cyber-criminals, or who gives safe haven to individuals or groups that conduct cyber attacks against another country, may be defined as a sanctuary state.[46] Policy-makers should seek to develop a common understanding of cyber-sanctuary states within the international community and intergovernmental organizations. Governments could apply diplomatic pressure or other actions to coerce the sanctuary state to exercise its duty to prevent cyber attacks against entities in other countries.

Deterrence of Cyber attacks

The National Security Strategy states that one strategic objective is to prevent cyber attacks.[47] But strategic documents and cyberspace initiatives focus on detecting and intercepting cyber attacks, with scant attention on developing methods to deter cyber attacks. Common arguments against the effectiveness of cyber-deterrence include the difficulties in accurately attributing the source of cyber attacks, the murky legal status of cyber attacks as an act of war, and the lack of

proportionate response options that carry sufficient weight to deter a cyber attack. Given the serious potential consequences of a successful attack against critical infrastructure, the United States should develop a robust defense strategy tailored to deter likely potential adversaries, include mechanisms for managing escalation during a cyber crisis, and give due consideration to complexities such as the presence of "patriotic hackers."

The central concept for deterring an adversary from taking action against the United States is to influence the adversary's decision-making calculus, with the result of inaction as preferable to action. The U.S. Joint Operating Concept describes three core concepts for deterrence: (1) pose a credible threat to impose costs to the adversary in the event of an undesired action, (2) deny the benefits to the adversary of the undesired action and (3) encourage restraint by offering consequences for inaction.[48] In the context of cyberspace, determining specific techniques to impose cost or deny benefits is complicated by the wide array of potential adversaries, which range from hackers set on breaking into sensitive systems for the sheer technical challenge, terrorist use of cyber attack as an asymmetric weapon, to nation-state use of cyber-espionage or cyber attack to support kinetic operations. The individual hacker's motivations and perception of risk are radically different from those of a nation-state. The United States must tailor effective approaches to deterrence based on a sophisticated understanding of the adversary's "unique and distinct identities, values, perceptions and decision-making processes."[49]

In developing tailored deterrence strategies, policy-makers must first identify the specific target(s) of the deterrence. A common perception holds that the difficulty of attribution (identifying potential or actual cyber attackers) arrests any meaningful attempt to develop cyber-deterrence. The relative ease of concealing one's identity within cyberspace does introduce uncertainty in attributing attacks in real-time. Decision makers must conduct deterrence planning within a larger geo-political context. Following the differentiated approach principle, deterrence should focus on potential high-end cyber attacks. Ongoing efforts to improve defenses may adequately deter low-end cyber attacks, such as hackers defacing websites. The high-end attacks

most in need of deterrence are likely to be conducted within the context of a political or ideological agenda. Terrorist groups, rogue states, and near-peer states such as China and Russia will continue to develop cyber power in the future. They will likely use cyber exploitation and cyber attacks as part of an overall strategy directed toward achieving political objectives.[50] Knowledge of potential adversaries and their motives and methods does not require real-time attribution during a crisis. Tailored deterrence strategies should be developed in peacetime for actors with known grievances against the United States. What America must avoid is facing a known cyber attacker without having an effective and proportionate response planned and reviewed. A cyber attacker would hope to catch the United States unprepared. A strong, declared policy, tailored to each important adversary, would begin the process of developing viable deterrence.

Should a non-state actor wish to remain anonymous, the difficulty of accurate attribution of the attack is a limitation to deterrence actions during a crisis. A non-state actor could launch a cyber attack from within a covering state without its knowledge, complicating efforts to identify the attacker. A criminal group might use a botnet, for example, to launch coordinated attacks from hundreds or thousands of computers located in multiple non-hostile countries.[51] A retaliatory response in cyberspace might damage networks in non-hostile countries or unrelated systems. If the perpetrator launched the attack from within a sanctuary state, the victim would likely have difficulty discriminating the degree of the state's involvement. One scenario is an attack launched with full approval of the sanctuary state authorities and carried out with state assets. Another possibility is an attack tacitly encouraged by the state but carried out with non-state assets. Responses would vary according to the degree of state involvement. The United States must bring intelligence and diplomatic resources to bear to complement technical attribution. In under-developed states with little cyberspace integrated into society, an appropriate cyber-response may not be available, reducing the range of options for policy-makers to economic, diplomatic or military responses.

The threat of retaliation (imposing costs) is the cornerstone of classical deterrence theory. Before considering options for retaliation, policy-

makers must determine the legal status of a cyber attack. CYBERCOM's commander affirmed that the "international Law of Armed Conflict, which we apply to the prosecution of kinetic warfare, will also apply to actions in cyberspace."[52] A full legal analysis of how the Law of War applies to cyber attack is outside the scope of this paper. But deterrence planning must include a decision-making structure at the national level to assess cyber attacks, determine their legal status as acts of war, and formulate a range of possible responses within the bounds of proportionality.

Deterrence by imposing costs or denying intended benefits to the attacker should consider all elements of national power, as well as actions purely in cyberspace, to calibrate a deterrent posture. Technical efforts to improve cyber defenses, by denying access to networks or deploying dynamic defenses to stop intrusions, may alter the adversary's cost-benefit analysis sufficiently to dissuade some cyber attacks, particularly less sophisticated adversaries with fewer cyber resources. When an adversary fails to penetrate a targeted system and cannot deliver the expected results, they must decide whether to accept additional risk by escalating the attack. Deterrence plans should deny benefits by developing ways to degrade the effectiveness of messages. As a "creative and cultural commons," cyberspace is increasingly becoming the "predominant domain of political victory or defeat."[53] An extremist cyber-attacker, for example, may judge an attack's effectiveness by how widely the ideological message spreads, captures publicity and lends some degree of credibility to the cause. Indirect effects could continue on blogs and forums long after the direct effects of a compromised system have been eliminated. A deterrence strategy should consider non-technical ways to neutralize the message, such as information operations and counter-messages. For significant cyber attacks, policy-makers should consider using other forms of national power, such as diplomatic and economic pressure. These may deter states who have the potential to employ cyber-weapons, or who might shield groups within their borders from launching cyber attacks. Government leaders could use these tools to offer incentives for adversaries to refrain from cyber attacks.

As with classical deterrence, cyber-deterrence planning should specify methods to manage escalation during a crisis, including transparency and signaling of intentions. A nation could in principle respond to a cyber attack with a kinetic counter attack, as a way to inflict unacceptable costs on a hostile opponent. Classical deterrence seeks to calibrate a response proportionate to the damage inflicted by an attack. For cyber-deterrence, the difficulty in discriminating indirect effects from direct effects and in linking physical damages with a digital attack clouds the ability to determine a measured and proportionate response. One might view a kinetic response as overly provocative and could result in undesired escalation of hostilities.[54] In conventional situations, adherence to international norms of behavior benefits stability, such as pre-announcing large troop movements, maritime "rules of the road,"[55] diplomatic engagement, and treaties and agreements that prescribe accepted behavior among nations. In contrast, legitimate cyber activities are completely intermingled with illegitimate cyber activities. A cyber attack may be difficult to distinguish from a cyber exploitation or hacker. Military use of cyberspace may be indistinguishable from civilian use. A culture of secrecy pervades U.S. cyber policies and compromises the ability to signal national intentions. The United States should pursue policies to make its cyber intentions and capabilities more transparent, while protecting its technical expertise. The United States must declare a strong policy of deterrence against cyber attacks in the National Security Strategy.

A workable framework for cyber early warning could assist in managing conflict escalation. Ned Moran, Professor at Georgetown University, proposed a useful five-stage model for helping to anticipate cyber attacks.[56] Stage 1 is recognition and assessment of latent tensions. Both state and non-state actors manifest background tensions long before actual attacks. States should assess tensions within a global geo-political context and with regard to capability to conduct cyber as well as physical operations. Stage 2 is cyber reconnaissance. Prior to initiating hostilities in cyberspace, adversaries are likely to probe one another, to discover vulnerabilities and strengths, just as adversaries would do on a conventional battlefield.[57] Stage 3 is the initiating event. In the 2007 Estonian cyber-war, the initiating event was the removal of the Soviet memorial in Tallinn. It caused tensions to boil over in

the form of riots in Moscow as well as in cyberspace.[58] Stage 4 is cyber mobilization. Following the initiating event, adversaries organize groups in cyberspace, recruit sympathetic supporters, and vet targets. For example, Chinese hackers mobilize support for political causes on message boards and chat rooms. In 2008, Chinese users created an anti-CNN forum to refute "the lies and distortion of facts from the Western Media."[59] Keen observation of internet forums and blogs combined with foreign intelligence gathering could identify when cyber soldiers are mobilizing and proactively raise the cyber alert status. Stage 5 is the cyber attack itself. The effectiveness of the attack depends on the sophistication of the perpetrators and the degree of reconnaissance and preparation performed. The United States should carefully observe the cyber activity of actors with known grievances against America, to look for signs of one of the five stages of the early warning model. Responses taken earlier in the process will more likely prevent escalation of the conflict to a more serious stage.

The presence of patriotic hackers will complicate efforts for deterrence and managing escalation during a conflict. As hostilities build, both sides of a conflict are likely to experience a surge of patriotic hackers, who act independently or in grass-roots groups to harass the opposing side. These activities are outside of government control but may be difficult to distinguish from a state-sponsored cyber attack.[60] The cyber war during the Russian invasion of Georgia in 2008 is an instructive example. A grassroots network of Russian hackers originated the StopGeorgia.ru project inside and outside the Russian Federation. Russia denied official involvement and direct support of the project, but it clearly benefited from the cyber attacks during the invasion and did nothing to stop them.[61] A more worrisome scenario could occur with a phenomenon known as "catalytic cyber conflict." This refers to a conflict where a third party instigates conflict between two countries by launching a cyber attack disguised to resemble one country attacking the other.[62] This occurred in July 2009 when a number of U.S. and South Korean government websites shut down over the Independence Day weekend. Suspicion immediately fell on North Korea, and one U.S. congressman even called for a military counter-attack. The likely perpetrator was not North Korea, however, but a hacker community in another country.[63] The incident underscores the fragility of stability in

cyberspace and the need for the United States to focus on major cyber threats from adversaries.

The Way Ahead

Protecting access to cyberspace serves U.S. vital interests. A comprehensive cybersecurity strategy, developed now while the United States is in a preeminent position in this newly evolving domain, will best use resources to solidify American cyber-power.

The U.S. government and military need policies to improve cybersecurity of critical networks and systems. Key conclusions and recommendations include:

- The United States should adopt a policy of differentiation among cyber attacks to prioritize response planning towards attacks that target more critical national assets.
- CYBERCOM and NSA's defense-in-depth of military and government systems illustrate an effective template for static and active cyber defenses.
- Industry should more broadly apply best practices for cybersecurity learned from CYBERCOM to critical civilian sectors.
- Initiatives under the CNCI show significant progress on creating a holistic, interagency approach to protecting government systems.

As cyberspace grows exponentially, the world becomes more interconnected and prone to shared vulnerabilities within cyberspace. The United States needs to exert international influence to encourage cooperation and collaboration to improve cybersecurity.

- Cultural differences about cyberspace present barriers to international cooperation, norms and responsible behavior within cyberspace.
- The United States should use diplomatic means to encourage wider acceptance of the principles promulgated in the Convention on Cybercrime.

- The international community should develop the concept of the cyber sanctuary state and pressure states who fail to prevent cyber attacks that emanate from within their borders.

Policy-makers should develop plans not just for improving cyber defenses but preventing cyber attacks by implementing initiatives that include tailored deterrence against known adversaries with cyber capabilities and tools to manage escalation during a cyber crisis.

- Deterrence planning need not wait for accurate attribution real time during a crisis, but rather should be developed within a broader geo-political context with regard to adversaries with known grievances against the United States.
- Attribution of non-state actors who wish to remain anonymous will be difficult. The state from which the non-state actor launches attacks may be complicit with the perpetrator, tacitly allow the attack or be completely unaware of the attack.
- The presence of patriotic hackers complicates deterrence planning and crisis escalation management.

More complete development of these approaches to a cyber strategy require study of the resources (means) to support the concepts (ways) discussed in this paper and to assess the degree of risk arising from identified gaps.

The importance of cyberspace to national security is growing with increasing band-width, faster computing power and greater reliance on digital networks to power critical parts of modern society. The U.S. cyber strategy must evolve to keep pace with innovative competitors to maintain freedom of cyberspace.

A Strategic Approach to Network Defense: Framing the Cloud*

Colonel Timothy K. Buennemeyer
United States Army

Agencies must focus on consolidating existing data centers, reducing the need for infrastructure growth…and increasing their use of available cloud and shared (virtual) services.[1]

—Vivek Kundra, U.S. Chief Information Officer

The U.S. Government has robust data networks that provide rapid transport of imagery, textual information, command and control data, and routine communications to support military operations and core business needs. This information is vital in the conduct of its ongoing war and peacetime missions. Historically, America's adversaries attempt to leverage network vulnerabilities to gain strategic advantage by exploiting information about U.S. military and commercial activities, trade secrets, financial information, system architectures, and myriad other data. The United States is arguably the most interconnected nation on earth and it plays a hegemonic role with regards to establishing and maintaining the rules that govern the Internet. Americans embrace digital technologies and desire greater interconnection for governmental, corporate, and personal utility.

This paper examines current Internet attack trends in the computer networking environment and proposes an enhanced framework for strategic system defense that is applicable to both corporate and Federal networks. The enhanced framework addresses these issues and assists in reducing the risks associated with assessing and adopting cloud computing. Computing clouds are large data centers filled with generic processing and storage facilities, operated as a single virtual computer or multiple reconfigurable servers.[2] Previously, cloud computing was basically the outsourcing of an organization's computing infrastructure.

** This paper was originally published by "Parameters" (Autumn 2011, Vol. 41, No. 3), and is republished here with their permission.*

Emerging cloud computing technologies will subsume existing enterprise networks and encompass system defenses that are typically designed, implemented, and managed at corporate information technology (IT) and regional processing centers. Once applications are logically extended through virtualization in a cloud computing environment, they are no longer tied to a physical location. The cloud service provider can develop dispersed support and hosting facilities that allow applications to perform as needed. The system user need merely access the typically web-based application to run any desired program.

The trend for networking infrastructures and computing centers is shifting toward consolidation for cost savings. Cloud computing provides for the outsourcing of entire networking and data centers, saving physical space, infrastructure, and labor costs. The prime benefit is the reduced cost of updating corporate information systems and infrastructures, which is transferred to the cloud computing provider.[3] Cloud computing is a major evolutionary leap forward in technology that virtualizes servers, infrastructures, and software as pay-for-use services. Leaders in the Federal government, and in particular the Department of Defense (DOD), have identified the significant benefits gained by adopting cloud computing, but they have not adequately considered the risks inherent with outsourcing information technologies.

Why Cloud Computing

Vivek Kundra, U.S. Chief Information Officer (CIO), proposes the Federal Government migrate its expansive computer networks away from a distributed architecture to a consolidated enterprise cloud computing architecture. In 2010, the White House initiated the Federal Data Center Consolidation Initiative (FDCCI) and issued guidance for the Federal CIO Council to have departments inventory their data center assets, develop consolidation plans, and integrate those plans into fiscal year 2012 budget submissions.[4] The FDCCI's goals are to: promote IT solutions that reduce energy and physical space usage; reduce the cost of data center hardware, software, and operations; increase IT security posture; and shift investment to efficient computing platforms that will

lead to closing 800 data centers by 2015.[5] Based upon this proposed migration, an expanded defensive framework that includes the evolving cloud computing environment, built on accepted network security principles, is critically needed. This expanded defensive framework would assist enterprise networking and cloud computing architects to better design more secure communication systems.

In terms of systems, the initial capabilities that are migrating to cloud computing environments are electronic mail, content archiving, and Software-as-a-Service (SaaS) applications. All benefit from consolidation into a virtualized cloud computing environment because these capabilities tend to require relatively low processing cycles on servers. However, there is a migration paradox with some IT capabilities. Computationally high cycle rate applications, transactional databases, and financial systems are ill-suited for cloud computing due to regulatory requirements. Interestingly, the cloud environment provider will update and manage their physical servers; however, organizations that employ their own virtual servers in a Platform-as-a-Service (PaaS) configuration will still be required to maintain and secure their own virtual systems. The implication is that if an organization is already lacking in their security regime, then migrating to a cloud environment will not necessarily improve their security posture. Lastly, government budgets are shrinking, so IT and data security investments must accomplish more at less cost. Adopting cloud computing is no panacea but may assist in accomplishing these efforts.

Cyberspace, Information Assurance (IA), and Network Defense

Cyberspace is defined in Joint Publication 1-02 as "a global domain within the information environment consisting of the interdependent network of IT infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."[6] Cyberspace is a contested domain, and the nation is "vulnerable to threats posed in cyberspace, while at the same time, dependent upon unfettered access."[7]

Internet proliferation is exponentially expanding across the globe bringing diverse people into an ever more interconnected cyber world. Based on Moore's Law, cyberspace should continue to expand, doubling

every two years with no upper limit in sight. The combination of easily affordable IT and rapidly expanding interconnectivity are changing the way that government, business, and individuals think, interact, and work.[8] The networks provide the means to rapidly share information making cyberspace, in a broader sense, a global commons for electronic information in the same fashion that the high seas are a global commons for maritime trade.[9] Thus, cyberspace is truly international and available for all to use. It is a shared resource that is loosely governed, routinely navigated via myriad uncharted routes, and, of increasing concern, often not well-secured.

With cyberspace quickly becoming a new global commons and rapidly growing under volatile, uncertain, complex and ambiguous conditions, governments, businesses, and individuals need to balance the information triad of confidentiality, availability, and integrity as part of a stable information security model. *Confidentiality* is the term used to describe preventing the disclosure of information to unauthorized individuals or systems. In information security, *integrity* means that data cannot be modified undetectably.[10] For any information system to serve its purpose, data must be *available* when it is needed. This model is known as the *CIA Triad* of IA, as shown in Figure 1.

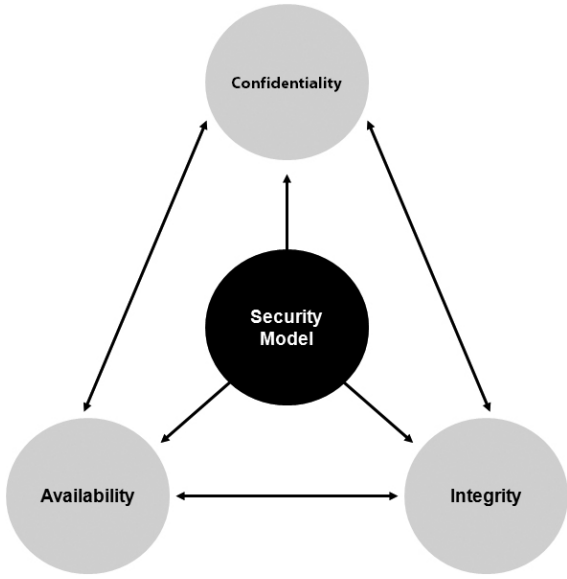

Figure 1. CIA Triad[11]

Security models are of critical importance in today's interconnected world, because information is routinely stored in large data centers that provide continuous access at the speed of electronic transfer. At the basic architectural level, there are systems hardware, software, and communications that must be protected. In this security model, confidentiality, integrity, and availability are often at the extremes of the triad and tradeoffs can potentially frustrate each other, so system designers must endeavor to find equilibrium among them. Favoring any one design direction over the other(s) may compromise the integrity of the other triad pillars. This means for computing systems used to store and process the information, the security controls used to protect it, and the communication channels used to access it must function well and be in balance within this security model.[12]

DOD Directive 8500.01E establishes roles and responsibilities, procedures, and processes while defining the components of the CIA Triad.[13] IA is the means by which IT managers attempt to protect, maintain, and provide IT security to their organization through the training, testing, and constant monitoring of controls implemented to secure an information resource.[14] IA offers measures that defend information by ensuring availability, integrity, authentication, confidentiality, and non-repudiation, while providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.[15] With today's networks, these IA defensive measures are implemented through a *Defense-in-Depth* framework of layered security that extends from the network to the endpoint computer. These need to be expanded further to reduce risk more effectively in emerging cloud computing environments, while addressing Internet attack vectors and vulnerabilities that threaten the global information commons.

Framing the Strategic Environment of Cyberspace

Attacks in cyberspace are fast and can simultaneously target a precise or a broad spectrum of systems. Attackers are often anonymous with few concerns about attribution. The instantaneous nature and the ability to attack the entire domain simultaneously are characteristics that make

cyberspace potentially a more dangerous and vulnerable environment for the unprepared than traditional warfighting domains.[16]

The U.S. Government identified the IT sector as an area of the nation's critical infrastructure and aligned its protection through the Department of Homeland Security (DHS) in 2009.[17] According to the National Academy of Engineering in Washington DC, cyber systems are the weakest link in our national security.[18] An example is System Control and Data Acquisition (SCADA) systems that manage critical utilities, such as electrical grids, water, sewer, and gas systems for regions, states, and local communities. Older SCADA systems incorporated limited security because they operated on closed communication systems, but most modern SCADA systems use the Internet to pass control information.[19] SCADA systems are potentially exposed to asymmetrical attack from our adversaries, which could undermine U.S. capabilities and its networks.[20] On average, it is estimated that 24 hours of SCADA down time from a major attack would cost $6.3 million with costs being the highest in the oil and gas sectors.[21] SCADA attacks are serious because direct control of operational systems could create the potential for large scale power outages or man-made environmental disasters.[22] SCADA systems are vulnerable, so greater efforts are required to design and place SCADA systems in more secure architectures.

Over the years, various commissions have examined cyber security and focused their efforts on SCADA systems, communications, financial networks, and other infrastructures. Reports conclude U.S. critical infrastructures are increasingly dependent on information and communication systems, and that dependence is a source of rising vulnerabilities.[23] In 2003, Presidential Executive Order 13286 required the United States protect against "disruption of the operation of information systems for critical infrastructure and help to protect the people, economy, essential human and government services, and national security of the United States, and to ensure that any disruptions that occur are infrequent, of minimal duration, and manageable, and cause the least damage possible."[24] IT is crucial to every aspect of modern life, and a serious attack could cripple systems for emergency services, military use, health care delivery, and electrical power generation.[25] Thus, a cyber campaign would almost certainly be

directed against the country's critical national infrastructure that would cross boundaries between government and the private sector, and, if sophisticated and coordinated, would have both immediate impact and delayed consequences.[26]

According to the U.S. Computer Emergency Readiness Team (US-CERT), cyber threats against the United States are broadly categorized into five potentially overlapping groups, consisting of national governments, terrorists, industrial spies and organized crime groups, hacktivists and hackers.[27] Any of these threat groups can have significant impacts against U.S. communication and SCADA systems, and consequently our infrastructure. Of greatest concern are national-level cyber warfare programs that pose threats along the entire spectrum of objectives that might harm U.S. interests.[28] Among the array of cyber threats, only foreign government-sponsored programs are developing capabilities with the future prospect of causing widespread, long-duration damage to U.S. critical infrastructures.[29]

Traditional terrorist adversaries of the United States, despite their intentions to damage U.S. interests, are less developed in their computer network capabilities and propensity to pursue cyber means than are other types of adversaries.[30] They are likely, therefore, to pose only a limited cyber threat. The United States should anticipate that more substantial cyber threats are possible in the future as a more technically competent generation enters the ranks.[31] International corporate spies and organized crime organizations with profit-based goals pose a medium-level threat to the United States through their ability to conduct industrial espionage and large-scale monetary theft, as well as their ability to hire or develop hacker talent.[32] According to the US-CERT, hacktivists form a small, foreign population of politically active hackers that includes individuals and groups with anti-U.S. motives. Motivated by propaganda and money rather than damage to critical infrastructures, hacktivists seek to achieve notoriety for their political cause.[33] Although the most numerous and highly publicized cyber intrusions are ascribed to individual hacking hobbyists, they pose a negligible threat of widespread, long-duration damage to national-level infrastructures.[34] The large majority of hackers do not have the motive or requisite tradecraft to threaten difficult targets such as critical U.S.

networks. Nevertheless, the large worldwide population of hackers poses a relatively high threat of an isolated or brief disruption causing serious damage, including extensive property damage and loss of life. As the hacker population grows, so does the likelihood of a highly skilled and malicious hacker attempting and succeeding in such an attack.[35]

According to Symantec, the United States was the top-ranked country for malicious activity, accounting for 23 percent of all attacks, as shown in Table 1.[36] It is apparent from this report that malicious activity is prevalent in the developed and rapidly developing nations of the world, and that attacks can cross all traditional boundaries regardless of governmental, commercial, economic and individual affiliation. The Internet is a permissive commons and as a consequence, so is its associated malicious actors, activities, and threats.

Rank	Country/ Region	Percentage	Malicious Code Rank	Spam Zombies Rank	Phishing Website Hosts Rank	Bots Rank	Attack Origin Rank
1	United States	23%	1	3	1	2	1
2	Brazil	6%	6	2	10	3	3
3	India	6%	2	1	30	20	8
4	Germany	5%	11	5	3	4	7
5	China	4%	3	28	7	6	2
6	United Kingdom	4%	4	7	4	9	4
7	Taiwan	4%	23	12	15	1	9
8	Italy	4%	21	11	11	5	6
9	Russia	3%	15	9	8	16	5
10	Canada	3%	8	41	2	17	12

Table 1. Malicious Activity by Country and Region[37]

While non-state sponsored computer network exploitation poses a serious risk to U.S. national security, those exploits are less troubling when compared to a nation-state threat, such as that of China, which seeks to go beyond cyber espionage in order to achieve military effects in future cyberspace.[38] Typically, specific information about attacks against

U.S. Government networks, attribution, and successful penetration is classified, so only representative open-source information is examined, such as that in Table 1. However, from the discussion about SCADA attacks, one can surmise that military effects, from a shutdown of regional power generation systems and distribution networks to data theft, are plausible examples across a broad range of realistic possibilities. As cyber technology becomes increasingly integrated into all facets of civilian and military life, U.S. national security planners see its pervasiveness as both a target and a weapon, similar to other capabilities and forces; so from this perspective, it is the one critical component upon which many modern societies depend, a dependence that is not lost on potential enemies.[39]

Why Network Defense Matters

Dennis Blair, former Director of National Intelligence, stated that "the cyber criminal sector, in particular, has displayed remarkable technical innovation with an agility presently exceeding the response capability of network defenders….Criminals are collaborating globally and exchanging tools and expertise to circumvent defensive efforts, which makes it increasingly difficult for network defenders and law enforcement to detect and disrupt malicious activities."[40] Internet-related economic losses reached $42 billion in the United States and $140 billion worldwide in 2008, while globally, companies could have lost over $1 trillion worth of intellectual property due to data theft.[41] Stolen trade secrets, proprietary research and development information, lost royalties, patent and copyright infringement, and financial information comprise the growing magnitude of data loss due to Internet-related theft. Thus, a brief examination of defensive capabilities to protect U.S. cyberspace is necessary. Figure 2 (following page) presents the classic security "onion" diagram employed in IT environments. It focuses on traditional physical, procedural, technical and personnel security that impact on the core IT components of data, applications, hosts, and networks.

Over time, more robust defensive constructs evolved to better protect information, servers, systems and transport communications. As newer capabilities are brought to the marketplace, defensive technologies

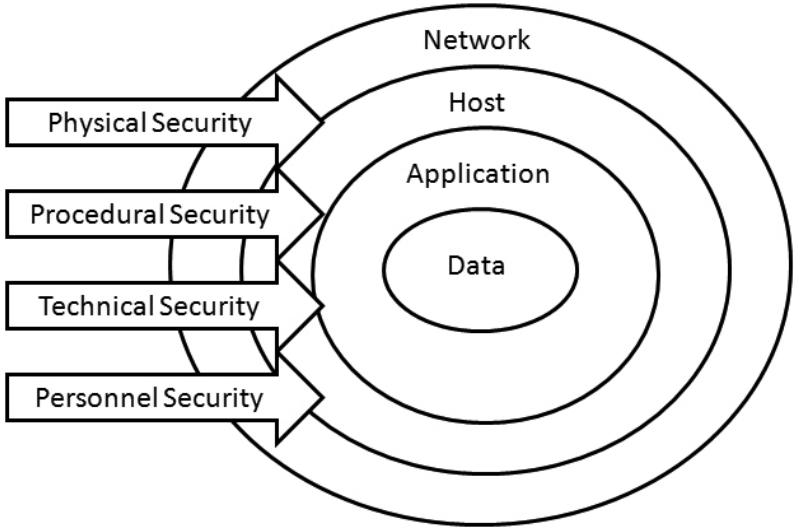

Figure 2. Classic Security "Onion"

adjust and adapt to the changing environment. Previously, technology companies sped new capabilities into the marketplace and security measures followed as an afterthought. This circumstance frequently left significant security gaps in organizational cyber environments. In today's environment, security is a basic design consideration when products and systems are proposed. Information technologies that lack defensible capabilities are doomed to fail the user, company or government employing them. A more modern information security construct is presented in Figure 3. While this security construct is not all inclusive, it is representative of the defense-in-depth concept that will continue to evolve as new capabilities and media enter cyberspace.[42]

McAfee, a trusted leader in the computer security industry, surveyed over 1,000 businesses. Their research has national security implications which indicate that substantial amounts of vital digital information, such as intellectual property and sensitive customer data, is being transferred between companies and continents and subsequently lost.[43] The report concludes that companies lost on average $4.6 million worth of intellectual property in 2008.[44] It is difficult to evaluate the total financial losses to businesses because companies are reluctant to

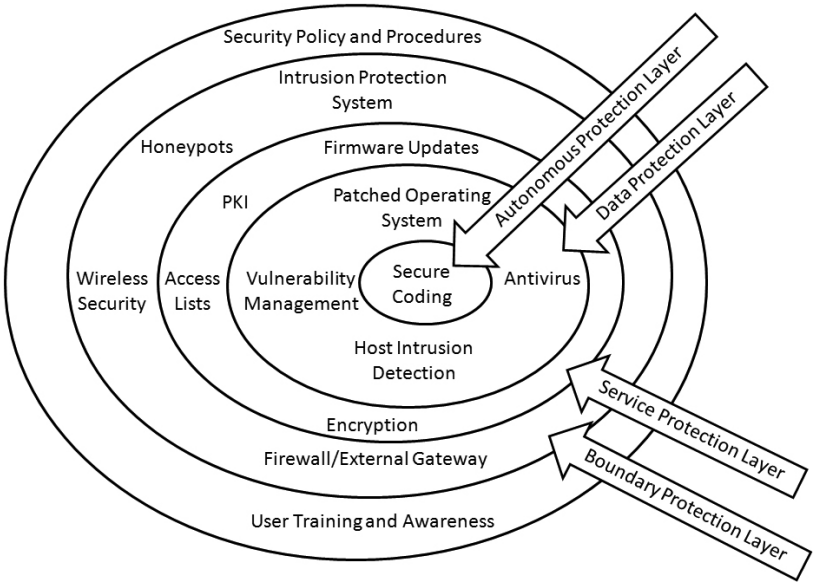

Figure 3. Modern Layered Defense Adapted from DHS Cyber Defense Strategy[45]

accurately report the figures due to concerns over losing consumer confidence. It costs an average of $600,000 per firm to respond to each security breach concerning the loss of vital information, which reflects just the reported costs of cleanup such as legal fees, victim notifications, but not infrastructure costs associated with prevention and detection.[46] The research further revealed that respondents worried more about their company's reputation due to public relations damage and information leakage than about the financial impact.[47]

An assumption is that migrating an organization's systems and capabilities to a cloud computing environment does not forgo the necessity to appreciate the changing nature of the cyber threat; nor does it allow for the abdication of security maintenance responsibilities by the data owner. Cloud computing does not change the defensive means available to security specialists. However, protection of the physical computers becomes paramount in a cloud computing environment. If the physical server is compromised, then the hosted virtual computers will likely all be compromised as well. The reverse is not necessarily the case. This places a heightened focus on the provider's abilities to

protect the physical servers, the center of gravity, in a cloud computing environment. Statistics indicate that one-third of breaches result from lost or stolen laptop computers and from employees accidentally exposing data on the Internet with nearly 16 percent due to insider theft.[48] When a user logs out from cloud computing services, however, the browser can be set to flush automatically, leaving nothing on the desktop to be lost or stolen. Therefore, security concerns with cloud computing are more a cultural issue associated with outsourcing than on any proven design weakness.[49]

Cloud Computing Defense Examination

Due to the implications to broad U.S. interests, a cyber security framework for cloud computing should be developed to actively shape protection efforts for U.S. cyber infrastructure, communication systems, and commercial, financial, and especially military networks from a broad range of crippling attacks and exploitive threats. Failure to protect U.S. governmental, military, and commercial networks could lead to the loss of intellectual property, trade secrets, and more. The compromise of these crucial networks would create chaos in banking, governmental, and military systems.

Traditionally, a defense-in-depth approach is applied to securing physical IT environments. This defensive approach may be less than adequate for cloud computing environments because systems are virtual and potentially mobile. Additionally, the instantaneous nature and the ability to attack the entire cyber domain make it potentially vulnerable.[50] Physical borders are important because cloud providers select their sites based on economic, connectivity, power availability and security criteria, but they have to make special arrangements among countries where data-movement restrictions apply.[51] Securing present day networking architectures with physical infrastructure provides known system environments to defend. However, cloud computing environments require additional risk consideration because the capabilities, data, and software are virtualized, while the physical infrastructure is out-sourced and may reside outside the trusted governance laws of a country.

A growing number of people believe cloud computing presents a paradigm shift in computing, on a par with the development of mainframes, personal computing, client-server computing and the Internet.[52] However, system owners are generally risk adverse, so adopting cloud computing as a solution requires a comprehensive defensive framework to ensure security. While cloud computing services are currently being used, experts cite security, interoperability, and portability as major barriers to further adoption.[53] Conversely, senior IT leader expectations are for enabling cost savings and an increased ability to quickly create and deploy enterprise applications.[54] This is where current policy and subsequent security framework is lacking. The National Institute of Standards and Technology is leading the development of standards for security, interoperability, and portability for the U.S. CIO by working with other agencies, industry, academia and standards development organizations to correct this circumstance.[55] The expectation is that well-defined standards will shorten the adoption cycle, enabling cost savings and an increased ability to quickly create and deploy enterprise applications.

Additionally, a government-wide risk and authorization program for cloud computing will allow agencies to use the authorization by another agency with the aim to drive to a set of common services across the government supported by a community, rather than an agency-specific risk model.[56] This effort is important because it will reduce the staff's burden in performance of lengthy IA certification and accreditation of applications and systems for greater cost efficiency.

Network State-of-the-Art Risk Framework

Industry-wide IA best business practices and computer defensive measures are not uniformly implemented, so a framework is necessary to assist with prioritizing and coordinating these defensive efforts. From a defense-in-depth perspective, cyber security is not just about deploying specific technologies to counter certain risks, as such; an effective security program for any organization will depend on its faithfulness and willingness to accept security as a constant constraint on all cyber activities.[57] The critical aspect for cloud computing environments is to understand what the new and inherent risks are and

how the change in service delivery might be affected. Risk assessments are a key cornerstone in defining, understanding, and planning remediation efforts against specific threats, potential vulnerabilities and architectural design flaws.[58] Thus, the establishment of an enhanced defensive framework for cloud computing environments is prudent.

According to the DHS, a defense-in-depth framework at a minimum should include the following areas:

1. Know the security risks that an organization faces
2. Quantify and qualify risks
3. Use key resources to mitigate security risks
4. Define each resource's core competency and identify any overlapping areas
5. Abide by existing or emerging security standards for specific controls
6. Create and customize specific controls that are unique to an organization[59]

Understanding that a framework is a guide for assessing risk, the basic framework is a valuable starting point. In a more traditional layered defensive construct, the systems tend to be collocated in a single or relatively close proximity networking or area data processing center, which is often managed and controlled by the system and data owner.

The challenge for incorporating more secure cloud computing is twofold. First, the owner's data and systems are often outsourced to an external cloud computing environment provider, so the owner no longer sets the environment's security policy or maintains its security posture. Second, cloud computing environments are established in multiple locations that are virtually interconnected. Its physical servers are often located in geographically inexpensive areas in terms of labor and governmental regulation.

By entering into a cloud computing environment, there are significant benefits to an organization through the reduction of its organic technical staff, which may free up capital for other uses. The downside is that the governance of the cloud environment is not transparent, so the service and data owner could unknowingly inherit higher risk for intrusion from the provider. Once an organization outsources its

technical support, it is difficult to reestablish organic technical skill sets. Simply stated, it takes years to develop institutional knowledge and then be able to apply that knowledge toward technical solutions for an organization. However, cost savings is often the driving force for adopting cloud computing. The key technical benefits are scalability and flexibility that allow an organization to pay for cloud computing resources as needed. An example of scalability comes from the private sector when their cloud computing environment allowed for a rapid response as demand jumped from 25,000 to more than 250,000 users in less than a week.[60] Because of the cloud computing technology, the company was able to scale from 50 to 4,000 virtual machines in three days to support the increased demand.[61] This capability would take significantly longer under our current construct. Lastly, if the cloud service provider provides secure services, then the users of those capabilities will be well-served. Ultimately, the adoption of cloud computing comes down to costs, technical staff capabilities, risks, and benefits. Those factors have to be weighed carefully when making the correct decision to migrate to cloud computing or not.

Enhanced State-of-the-Art Risk Framework for Cloud Computing

Due to the tendency for outsourcing of the cloud computing environment, this paper proposes to add five additional areas to the existing defense-in-depth framework. Below are the proposed areas:

1. Assess the security posture of the cloud computing environment
2. Know the physical location of the actual cloud computing center(s)
3. Understand your service-level expectation relative to perceived risks
4. Assess applicable governance, laws, regulations and policies
5. Know your tolerance for service interruption, data loss, and recovery

With these additional framework layers, organizations will be able to better assess their information security posture. Risk assessment is a cornerstone in prudent system design. Having an accurate and well-documented architecture and complementary risk assessment empowers an organization to be more security conscious, deploy effective security

countermeasures, and be equipped to understand security incidents more readily.[62] In cloud computing the service provider establishes the cloud's architecture, security posture, and provides the service delivery. However, it is incumbent on the organization as the service and data owner to fully appreciate and assess all the environmental risks.

Cloud computing environments are a new frontier with very few specific legislative standards for security or data privacy, and there is limited governance because laws lag behind the technology development.[63] In the cloud computing environment delivery of capabilities fall into two broad categories: SaaS and PaaS. Providers herald the robustness of their systems, often claiming that cloud environments are more secure than existing enterprise environments, but the facts are that any security measure ever breached was once thought to be infallible.[64] At present, security is imbued in the cloud computing environment, but the level of defensive measures and their implementation may vary significantly between providers.

Applicability for U.S. Federal Enterprise Environments

Arguably, the DOD operates one of the larger and more robust enterprise computing environments in the world. Then Secretary of Defense, Robert Gates, in his January 2009 testimony before congress stated, "With cheap technology and minimal investment, current and potential adversaries operating in cyberspace can inflict serious damage to DOD's vast information grid – a system that encompasses more than 15,000 local, regional, and wide-area networks, and approximately 7 million IT devices."[65] Although the DOD's network structure is linked, the military services and agencies typically operate distinct domains, so it would require a vast financial and labor effort to migrate to a cloud computing environment. The consolidation effort will also drive the military services to examine IT investments from a Title 10 perspective, which may limit their autonomy with regard to their mandate to man, equip, and outfit their forces. This migration will likely occur incrementally over the next 5-10 years and may allow for the recapitalization of hundreds of millions of dollars in network operating funds. As shown in Table 2, the DOD currently spends over $36.3 billion annually for IT, according to the IT Dashboard.[66]

This dashboard provides the public with online details of U.S. Federal Government IT investments based on Federal agencies' monthly reports to the U.S. Office of Management and Budget.[67]

Bureau	Total FY2011 Spending (Billions)	No. of Total Investments
Department of the Army	$7.30	256
Department of the Air Force	$6.80	651
Department of the Navy	$7.60	789
Department of Defense Agencies	$14.60	536
Department of Defense (Total)	**$36.30**	**2232**

Table 2. U.S. DOD IT Portfolio Budget for FY2011[68]

The Federal government, as part of a broader IT transformation, needs to fundamentally shift its mindset from building custom systems to adopting light technologies and shared solutions.[69] This is necessitated because departments and agencies typically build systems that duplicate capabilities and lack integration within the government, causing unnecessary IT redundancies and increased costs. An example is the explosion in the number of Federal data centers from 432 in 1998 to 2,094 in 2010 that highlights this ongoing IT expansion.[70] With a subjective examination of the DOD IT expenditures juxtaposed across the Federal Government above, one can sense the potential cost savings in the billions of dollars by eliminating IT redundancies, consolidating server farms and data centers into cloud computing environments, and the reduction of technical staff.

Information services should enable the departments and agencies to better serve the American people. Despite spending more than $600 billion on IT over the past decade, the Federal government has achieved little in terms of the productivity improvements that private industry has realized from IT.[71] This reflects the growing dependency on information systems by Federal employees to accomplish their daily work. Unless checked by a transition to cloud computing, this IT growth trend will persist and expand. However, the National Security Agency, like other Federal agencies, is trimming its spending on IA from $915 million in 2010 to $902 million in 2011.[72] It is likely this

trend of reducing expenditures for IT security will continue across the Federal government as budgets tighten.

IT projects often run over budget, fall behind schedule, or fail to deliver promised functionality because a project designer's approach simply aims to deliver full functionality in a few years, rather than modularizing projects into more manageable chunks and demanding new functionality every few quarters.[73] This circumstance is complicated because of the reliance on proprietary application and system designs when cloud computing solutions might suffice. This amounts to a change in mindset as well as an adjustment to the key functions of management and staff of the IT efforts. If cloud computing is the next generation environment, then substantial training of technical staff will be required. Although there will likely be reductions in some technical staffing areas, such as server system administrators, network maintenance and monitoring personnel, and router and gateway administrators, there will likely be increases in application and data developers. Undoubtedly, these increases will be less than offsetting, so organizations can anticipate some overall reduction in technical staff. Once gone, that knowledge will be difficult to replace. Lastly, technical staff often helps to translate executive and senior leader ideas into automation realities, so the net loss of technical staff may impede some automation understanding because of the presumed reduction of computer savvy staff.

Future IT Security Challenges

The 2010 Joint Operating Environment (JOE) indicates that "the globe-spanning range of cyberspace and its disregard for national borders challenge our legal system and complicate our ability to deter threats and respond to contingencies."[74] This recognizes that information shared across networks continues to increase while concurrently reshaping our society. The concept of having borders in cyberspace loosely exists, but this is reflected as physical network domain borders for enclaves or as publically and privately facing world wide web pages as well. Traditionally, laws in many countries recognize sovereign borders, but this Westphalian concept is difficult to enforce in cyberspace. An example is the *Safe Harbor* agreement between the U.S.

Department of Commerce and the European Union that attempts to bridge the gaps between the numerous privacy laws and regulations over the cross-border flow of personal information.[75] It allows companies to share information, while avoiding interruptions in their business dealings or facing prosecution by authorities under European privacy laws.[76] The problem with this type of agreement is enforcement. Thus in nine years, the U.S. Federal Trade Commission obtained consent decrees that prohibited only six U.S. companies from misrepresenting privacy and security compliance but never imposed any penalties.[77] Therefore, data sharing on the Internet permeates sovereign borders, but laws governing commerce data are specific to each country. This circumstance poses a growing challenge for implementation of cloud computing environments that may potentially handle regulated and other sensitive data between multiple countries.

Future security threats will challenge lawmakers, strategists, businessmen and technologists to develop new approaches to operating in cyberspace. According to the JOE, there are no protected zones or rear areas in cyberspace because all are equally vulnerable.[78] As airpower transformed the World War II battlefield environment, cyberspace permeates physical barriers that shield a nation from attacks on its commerce and communication.[79] Moreover, there is some expectation that future wars will include cyberspace as a prime venue for frontline and asymmetric operations and conflict resolution. This places information managers in a reactive position to develop countermeasures for new attacks. Once feasible defenses are established, attackers will continue to devise new methods to gain access. The challenge for defenders is that there are thousands of flaws an attacker can exploit, but the attacker only needs to find one that works to succeed.

The U.S. Government Accountability Office's (GAO) Director of Information Security Issues, Gregory Wilshusen, testified that "the four most prevalent types of incidents reported to the US-CERT during fiscal year 2009 were: (1) malicious code comprising 23 percent; (2) improper usage, 20 percent; (3) unauthorized access, 16 percent; and (4) unconfirmed incidents under investigation, 36 percent."[80] He also stated that "GAO and agency inspectors general reviews continue to highlight deficiencies in the implementation of security policies and

procedures at Federal agencies."[81] The predictions seem rather clear that sophisticated attacks will continue to target emerging capabilities in cyberspace, while the trends continue regarding the lack of compliance on the part of governmental agencies to address security threats.

Conclusion

This research examined the challenges associated with providing network defense in the current enterprise environment and recognizes that consolidation of area processing and networking centers into cloud computing environments is the likely future migration path. The primary reasons for adopting a cloud computing environment are rapid scalability and flexibility with SaaS and PaaS. There is a perception that migration to the cloud computing environment will also yield cost savings through reduced physical infrastructure and technical staff. While the reality of reduced physical infrastructure will occur, it is not clear that the technical staff will be significantly reduced because virtualized servers still need to be maintained. Additionally, this paper proposed an enhanced defensive framework to better assess the risks of cloud computing. While the existing framework is still valuable, the added assessment areas address and capture the dynamic nature of the cloud computing environment and afford the system owner improved attack risk mitigation through a more complete assessment of the environment.

The JOE predicts that network connectivity will grow by 50% a year, providing about 100,000 times more bandwidth in 2030 than today; and computers will run one million times faster, so a home computer would be capable of downloading the entire Library of Congress (roughly 16 terabytes of data) in 128 seconds.[82] With these predictions in mind, it is apparent that security challenges and attack sophistication will increase proportionally. The greatest concern for government and businesses is to be lulled into a false sense of security by adoption of cloud computing environments. The benefits are equally apparent, but the consolidation of multiple virtual machines into an outsourced cloud computing environment incurs some risk. If the physical server fails, then the numerous virtual machines will go silent. Equally, if the physical server is compromised, then the hosted virtual computers

will likely be as well. Ultimately, it boils down to data owner risk, expectations, and tolerance of not controlling their systems.

An appropriate defense requires commitment, careful planning, and systematic implementation incorporated into cyberspace's virtual world, if there is any chance of limiting damage in the real world.[83] The defense of virtual computers is more akin to holding atmosphere in your hand or cyberspace as the case may be. Clausewitz stated, "The defender is at greatest disadvantage when compelled to protect a wide area against multiple axes of advance. In this instance, the attacker using surprise may throw his full strength at any one point."[84] Conclusively, the network defense employs substantially more means to preserve security in computing environments, so the attacker may actually have the initiative and an asymmetric advantage in cyberspace. However, well-designed cloud computing environments may change the balance back in favor of the defense, while reducing costs and improving service.


U.S. ARMY WAR COLLEGE
Prudens
Futuri
Carlisle Barracks, PA

Crime or War: Cyberspace Law and its Implications for Intelligence

Colonel Bryan D. DeCoster
United States Army

Our Nation's growing dependence on cyber and information-related technologies, coupled with an increasing threat of malicious cyber attacks and loss of privacy, has given rise to the need for greater security of our digital networks and infrastructures. In the Information Age, the very technologies that empower us to create and build also empower those who would disrupt and destroy.

—Barack Obama, *Proclamation*, National Cybersecurity Awareness Month, 2009

This statement by U.S. President Barack Obama highlights current national security concerns with cyberspace, which is "a global domain…consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."[1] In 2003, U.S. President George W. Bush published *The National Strategy to Secure Cyberspace*, and in 2009, President Obama directed a 60-day review of cyber-security strategy which resulted in a policy review document.[2] Both documents recognized that cyberspace was a new domain in national security with complex legal issues and network vulnerabilities, especially in the nation's critical infrastructure.[3] Since cyberspace is relatively new, existing international law does not directly distinguish between crimes and acts of war for activities in cyberspace. However, making the distinction between crime and war is essential in determining which of the multiple stakeholders takes the lead in preventing or responding to computer intrusions on United States government or private networks.

Defining the evolving terminology related to cyberspace is part of the challenge in making legal distinctions. This paper uses the definitions accepted in joint doctrine with some minor modifications.

Computer intrusions are "incident[s] of unauthorized access to data or an automated information system"[4] or networks by state and non-state actors. Computer intrusions take two forms: computer network exploitation and computer network attack. Computer network exploitation (CNE) is "enabling operations and intelligence collection capabilities conducted through the use of computer networks to gather data from target or adversary automated information systems or networks."[5] Computer network attacks (CNA) are "actions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves."[6] While CNE and CNA tools are similar, CNE activities are usually conducted in support of espionage, while CNA activities are intended for profit, sabotage, or other harm.[7]

According to General Keith Alexander, commander of U.S. Cyber Command (USCYBERCOM): "There is a real probability, that in the future, this country will get hit with a destructive [cyber] attack, and we need to be ready for it."[8] Imagine the following scenario as an example of such an attack. It is 2012 and the United States has just fallen victim to a cyber worm designed to precisely target the supervisory control and data acquisition (SCADA) systems of nuclear power facilities and cause physical harm by shutting down reactor cooling systems. The worm infected 20 nuclear facilities, with two of the facilities experiencing temporary cooling system failures, resulting in 15 deaths and 80 injuries before the damage could be contained. Attribution has been elusive, with the worms being traced back to computers in the United States, India, and Pakistan. However, intelligence officials suspect Iran of being behind the worm as retaliation for a 2010 CNA against Iranian nuclear facility centrifuges.

A post-attack intelligence review by the Office of the Director of National Intelligence (ODNI) revealed several data points that were never shared or connected. The Central Intelligence Agency (CIA) estimated Iran had intent but insufficient capability for CNA. The National Security Agency (NSA) conducted a network analysis that showed contacts between Iranian intelligence officials and a Russian hacker website also associated with terrorist and criminal groups. The

Department of State (DoS) had a human intelligence (HUMINT) report of a highly skilled Russian hacker traveling to Iran two weeks prior to the attack. At this point in time, the USCYBERCOM and the federal government remain unclear on how to respond since attribution and the legal status of the attack remain unclear, whether the attack was a criminal act or an act of war.

This paper examines the law concerning cyberspace and analyzes six basic sources of cyberspace threats in order to propose which threats and their resulting computer intrusions are criminal as opposed to acts of war. The paper then describes the implications for intelligence collection and analysis that result from this legal and threat environment. These implications generate proposed imperatives for the intelligence community that could help prevent scenarios like the one described above.

Existing Law and Stakeholders Regarding Cyberspace Activities

There are differing opinions on the applicability of current international law to cyberspace. Some scholars and lawyers argue that there are "no common, codified, legal standards regarding cyber aggression" and "current international law is not well suited for cyber-attacks."[9] Others argue "that a considerable body of international law applies to the use of force by states in cyberspace."[10] Applying the general international laws on the use of force by analogy can help determine whether a computer intrusion is "simply a crime committed by a non-state actor or an unlawful use of force by a state under international law."[11] Advocates for new international laws to directly address computer intrusions argue that applying law by analogy to cyberspace is currently necessary but flawed for several reasons: translation problems, exclusion of non-state actors, and applicability of cyberspace to multiple overlapping legal regimes.[12] This paper uses the law by analogy argument since it appears to be the most generally accepted method despite its limitations.

So what international law is applicable by analogy? What constitutes an act of war in cyberspace? Making a legal distinction between crime and war is complicated due to the lack of accepted international definitions for key terms of aggression such as act of war, armed conflict, use of force, and armed attack. International laws and treaties, to include the

United Nations (UN) Charter, do not clearly define these terms of aggression.[13] In general, an act of war is any use of force occurring in the course of armed conflict. However, to apply this to cyberspace requires further examination of use of force, armed attack, and armed conflict within the context of international law.

Article 2(4) of the U.N. Charter prohibits the "use of force" against another state.[14] For the purposes of this paper, use of force is defined as "a state activity that threatens the territorial integrity or political independence of another state."[15] Customary international law prohibits a state from using force for retaliatory or punitive actions but allows using force in self-defense to deter future aggression. Article 51 of the U.N. Charter recognizes this right of a state to self-defense against an "armed attack."[16] For the purposes of this paper, armed attack is defined as "a use of force that rises to a certain scope, duration, and intensity threshold."[17] United Nations General Assembly Resolution 3314 provides examples of aggression that constitute armed attack, but they are traditional lethal examples as opposed to the non-traditional activities of cyberspace.[18] According to Common Article 2 of the four Geneva Conventions of 1949, armed conflict exists upon formal declaration of war; occupation of a state; or any other armed conflict between states even if war was not formally declared.[19]

To summarize and apply these terms, short of a formal declaration of war or occupation, armed conflict exists when one state uses force against another state that is of a scope, duration, and intensity that qualifies it as an armed attack.[20] Essentially, a use of force that meets the threshold of an armed attack qualifies as armed conflict and, under Article 51, triggers the right to self-defense.[21] Using law by analogy, a computer intrusion by one state against another state's computer network may qualify as a use of force if it threatens the territorial integrity or political independence of the state. If a state determines that another state's computer intrusion meets the threshold of an armed attack, the intrusion could also be considered armed conflict and an act of war.

The key distinction is the scope, duration, and intensity threshold for an armed attack. There is a requirement for legal analysis on a case-by-case basis to determine which computer intrusions meet the threshold

for an armed attack.[22] Essentially, lawyers must study state practice and international precedent to make legal determinations, applying existing law by analogy. Determining whether a state's computer intrusion is an act of war requires a legal interpretation that concludes "an activity not traditionally considered an armed attack [computer intrusion] is used in such a way that it becomes tantamount in effect to an armed attack."[23] Lawyers can use several proposed frameworks to determine when a computer intrusion equates to armed attack. These include the Schmitt framework, which applies seven factors beyond scope, duration, and intensity; and the Libicki framework, which categorizes armed attacks into groupings which are universally, multilaterally, or unilaterally accepted within the international community.[24]

Regardless of the framework applied, it seems to be generally accepted through law by analogy that a CNA conducted by a state that causes physical damage to another state's assets would meet the threshold for unlawful armed attack unless conducted in self-defense or as part of a U.N.-sanctioned operation.[25] A CNA used in self-defense under U.N. Charter Article 51, or as part of a U.N.-sanctioned operation, is legal as long as the principles of the Law of Armed Conflict are followed.[26] However, even if in self-defense, a CNA conducted by a state with the intent to cause physical damage to "works or installations containing dangerous forces, namely dams, dikes and nuclear electrical generating stations" would appear to be an unlawful armed attack under the 1977 Geneva Protocol I, Article 56.[27] For example, the CNA on U.S. nuclear power plants described in the opening scenario would be considered an unlawful armed attack if it could be attributed to a state.

At this point, it is important to note two additional limitations in international law. First, CNE would not generally meet the standard of a use of force or an armed attack. In 1960, the U.N. Security Council concluded that a U-2 reconnaissance flight by the United States over Soviet territory was not a use of force under UN Charter Article 2(4). Using this precedent by analogy, the "virtual penetration of a state's cyberspace" for reconnaissance (e.g., CNE) also does not constitute a use of force under U.N. Charter Article 2(4).[28] While CNE and espionage do not violate international law, they could be prosecuted as criminal activity if the domestic law of the state in which it occurs outlaws such

activity.[29] Second, international law and treaties, to include the U.N. Charter, apply to state-on-state conduct and exclude non-state actors. Therefore, in order to make a legal determination that a CNA qualifies as an armed attack, it must be attributed to a state. As was evident in the example scenario, attribution for computer intrusions is extremely difficult; even if attributed to an individual, proving that individual was acting in an official capacity for a state is doubly difficult.[30]

As noted above, CNE and the computer intrusions of non-state actors, to include CNA, could constitute crimes rather than acts of war, unless a U.N. resolution or other international convention were to specifically sanction military operations against non-state actors conducting CNA. CNE and the computer intrusions of non-state actors are customarily left to domestic law enforcement agencies or to states for resolution. A state's response against a non-state actor is a "law enforcement issue that must, at least at present, be principally addressed through cooperative bilateral and multilateral extradition and mutual legal assistance treaties."[31]

Domestically, the Computer Fraud and Abuse Act (CFAA) is the principal U.S. law addressing Internet-related computer crime.[32] The CFAA prohibits unauthorized access to a protected computer or gaining and using information in a manner exceeding authorized access. Robert Morris, a Cornell University computer science student, was the first person convicted under this act in 1990 when he released a virus that affected hundreds of educational and military computers during the early stages of the Internet.[33] Additionally, the United States has indicted criminals for using, maintaining, and selling botnets, which are networks of robotic internet devices that control other computers without the user's knowledge.[34] The use of botnets can be prosecuted as civil trespass but the plaintiff must establish damages as well as trespass in cyberspace.[35] There are also copyright laws protecting companies from cyber-theft. The Digital Millennium Copyright Act protects companies that encrypt trade secrets from hackers who would try to circumvent the company's encryption or digital locks.[36]

These U.S. laws apply to both U.S. and foreign citizens, but prosecution of foreign citizens is more difficult because it requires recognition of the law and the right to extradition by another state.

Prosecution of cyber-crimes that cross state borders, enforcement of national criminal judgments, and extradition of cyberspace criminals are complicated since "there is no international treaty for enforcement of judgments or any Convention providing for extraterritorial Internet enforcement."[37] Some nations have weak governments, security forces, or law enforcement agencies that would have difficulty capturing and extraditing criminals.

Most nations have different laws and some nations have no laws regarding cyberspace activities. For example, France made it a crime for an Internet service provider (ISP) to "give access to or possess Nazi memorabilia" while China required Yahoo to "filter materials critical of the Communist party regime as a condition of access to Chinese markets."[38] Both of these national rulings are at odds with U.S. rulings on First Amendment rights and cause conflicts in Internet governance since many of the ISPs are American-based. An Israeli citizen who hacked into the Rome Lab, a U.S. military research and development laboratory, multiple times in 1994 was not prosecuted because there were no Israeli laws recognizing this as a crime.[39] In 2000, a Filipino hacker was not prosecuted for his "I Love You" virus, which infected over 60 million computers worldwide, again because there were no laws against this cyberspace activity in the Philippines.[40]

There has been some recent international progress in trying to address these difficulties in accountability for cyber-crimes. Thirty-three countries, including the United States, have signed the Council of Europe's Convention on Cybercrime (CoECC) published in November 2001.[41] The Convention "seeks to better combat cybercrime by harmonizing national laws, improving investigative abilities, and boosting international cooperation."[42] Critics of the Convention point out, however, that it will be ineffective as long as the signatories do not include nations where criminals and terrorists operate freely.[43] The UN Secretariat has also recently established a Working Group on Internet Governance (WGIG) to study and make proposals for Global Internet Governance.[44]

A final complicating factor in this examination of when cyberspace activities qualify as crime versus war relates to the key stakeholders involved. There are many stakeholders with varied and often competing

interests and authorities. This further complicates the environment and makes the formulation of consistent, unified responses against cyberspace activities challenging.

Internationally, key stakeholders include multilateral cooperative organizations like the UN, CoECC, North Atlantic Treaty Organization (NATO), and International Criminal Police Organization (INTERPOL); non-governmental organizations (NGO); states; and non-state actors. Through its Security Council and General Assembly resolutions, the UN may sanction a state or non-state actor for a CNA that constitutes an armed attack or authorize military actions against state and non-state actors conducting CNA. NATO also has the authority to determine when a CNA on one of its member states constitutes an armed attack. For example, in 2007 NATO determined a CNA against Estonia did not trigger Chapter 5 thresholds requiring a NATO response against an attack on a NATO member.[45] The INTERPOL and the CoECC are focused on cooperation against cyber-crime. Some NGOs are very focused on privacy rights and argue against cyber-security measures that improve attribution methods on the Internet. State actors have varied interests; some want to advance cooperation against computer intrusions and cyber-crime, while others tend to exploit difficulties in attribution by employing covert non-state actors to perform their CNE and CNA. Non-state actors can act individually or in support of states when conducting computer intrusions.

Domestically, key stakeholders include: agencies of the Executive Branch such as the National Security Council (NSC), the Department of Defense (DoD), the Department of Homeland Security (DHS), the Secret Service, the Department of Justice (DoJ), the Federal Bureau of Investigation (FBI), the Federal Trade Commission, DoS, ODNI, CIA, NSA, and USCYBERCOM; members of Congress; NGOs and lobbyists; private companies; and governments and courts from federal to local level. The NSC advises the president on policy decisions, while Congress, state, and local governments pass laws related to cyberspace activities. Courts make rulings on law regarding cyberspace activities at all levels. Non-governmental organizations and lobbyists have varied interests from advocating privacy rights to increased federal

regulation of cyber security. Private companies own 85% of the nation's infrastructure, including the digital infrastructure, and are therefore invested in their own cyber security.[46]

Based on law and policy, acts of war in cyberspace involve the DoD, the ODNI, the CIA, the NSA, the USCYBERCOM and potentially the DHS, while cyber-crimes involve the DHS, the Secret Service, the DoJ, the FBI, and the Federal Trade Commission.[47] The DHS is responsible for focusing on protection of government agency and private information systems to include reducing and consolidating external access points, deploying passive network sensors, and defining public and private partnerships. The DHS is also the focal point for efforts to protect the nation's computer-reliant critical infrastructure.[48] The DoD is responsible for protecting military information systems to include monitoring, increasing security of classified networks, and deploying intrusion prevention systems. The ODNI is responsible for monitoring intelligence community information systems and other intelligence-related activities, including the development of a government wide cyberspace counterintelligence (CI) plan.[49]

Sources of Threats and Their Status Under Law

Having examined the law on cyberspace and key stakeholders, this paper will now describe the basic threats in cyberspace and their general status under the law. There are six basic sources of threats: foreign nations, criminal groups, hackers, hacktivists, disgruntled insiders, and terrorists.[50]

Foreign nations would appear to have the most robust cyberspace means and capabilities at this time. It is estimated that "over 120 countries already have or are developing computer attack capabilities."[51] Most of these countries are focused on CNE or using cyberspace tools as part of their intelligence and espionage activities.[52] According to the ODNI, the majority of computer intrusions originate in Russia and China, and both nations have large efforts focused on CNE and CNA.[53]

The CNE activities of foreign nations fall into the criminal category under existing law and are more common than CNA. Computer network attacks by foreign nations are generally accepted as the most

dangerous threat to U.S. computer networks.[54] As previously discussed, CNA could rise to the level of an armed attack based on scope, duration, and intensity. Essentially, a CNA that causes physical damage could equate to an armed attack. The primary difficulty, however, is attributing that armed attack to a foreign nation.

There are several historical examples of CNA believed to have been launched by foreign nations. In 1999, the Indonesian government was generally blamed for what might have been the first reported state-on-state CNA when non-governmental computers in Ireland were attacked, bringing down the East Timor virtual country domain and Internet service to over 3,000 customers.[55] In April and May 2007, Estonia was the target of the "first-ever coordinated cyber-attack against an entire country."[56] Estonia's digital infrastructure suffered extensive distributed denial of service (DDOS) and botnet attacks that adversely affected its banking and government operations and denied basic access to ISPs.[57] In August 2008, the country of Georgia experienced extensive CNA used in conjunction with conventional military attacks. As Russian troops were moving into South Ossetia, Georgia's digital infrastructure and government with websites experienced DDOS attacks, web defacement, and disinformation and propaganda attacks intended to paralyze the government response.[58] In June 2010, several countries discovered the first precision CNA intended to cause physical harm to infrastructure in the form of a cyber-worm known as Stuxnet. This cyber-worm targeted, infiltrated, and took control of specific SCADA software "used to run chemical plants and factories as well as electric power plants and transmission systems worldwide."[59] The worm was estimated to have infected at least 45,000 industrial control systems worldwide and may have been specifically designed to target centrifuges at the Bushehr Iranian nuclear facility.[60]

Debate continues in each case over whether there was sufficient physical damage and/or attribution to qualify the CNA as armed attacks by a foreign nation.[61] Attribution of a CNA to a foreign government is complicated because it is difficult to trace the connection between an individual hacker and a government. Furthermore, some nations may attempt to use an IP address that attributes the CNA to another nation or individual (i.e., they engage in false flag operations).[62]

Criminal groups, by the nature of their intent, fall into the category of cyber crime. These groups conduct computer intrusions for profit, and cyber crime will continue to expand as long as it remains lucrative.[63] Criminal groups target personally identifiable information (PII) of individuals and proprietary information from private companies in order to gain unauthorized access to credit and bank accounts, run scams, or sell information to the highest bidder. In some cases, these groups seize SCADA controls for extortion, forcing the private company to pay a fee to regain control of important functions.[64] Criminal groups also market and sell the tools for crime like botnets, spiders, and zombie computers.[65]

Hackers comprise a wide category of individuals who often conduct CNE and CNA for thrills or bragging rights.[66] In the past, hackers required exceptional skill, but the proliferation of attack scripts and protocols from the Internet available for download on hacker Web sites have made hacking easier. In general, "attack tools have become more sophisticated and easier to use."[67] Hackers generally fall into the category of cyber crime and are increasingly co-opted and paid for by criminal groups for their services. Hackers can also be co-opted by foreign intelligence services to perform CNE or CNA when a nation wants to prevent attribution. It is feasible that a hacker could conduct a CNA that rises to the level of an armed attack, but he would have to be pursued on a criminal basis unless attribution to a foreign nation could be proved. This would be the case from the opening scenario if the CNA were attributed to the Russian hacker and not the Iranian government.

Hundreds of hackers conduct computer intrusions each day. The previously cited example of Robert Morris is a typical example. In February 1998, two California teenagers and an Israeli teenager conducted CNA on DoD computers in intrusions known as *Solar Sunrise*.[68] In 2003, a hacker used the Slammer worm to corrupt the safety monitoring systems of a nuclear power plant in Ohio for five hours via a backdoor through the Internet.[69] Another hacker's worm, known as MS Blast or Blaster, was reportedly linked to the major power outage that hit the northeast United States in August 2003, where it "crippled key detection systems and delayed response during a critical

time."[70] While these computer intrusions by hackers took significant money, time, and other resources to fix, none rose to the level of an armed attack.

Hacktivists are individuals or groups who conduct politically motivated computer intrusions. They normally use DDOS attacks or modify publicly accessible Web pages or e-mail servers to send a political message.[71] Hacktivists fall into the criminal category. Russian hacktivists, incensed by Estonia's plan to move a Russian soldier monument, were involved in the 2007 CNA against Estonia. In the case of Estonia, the energized hacktivists made attribution for the attacks even more difficult than usual, possibly providing an effective smokescreen for Russian government operatives.[72]

Disgruntled insiders can work from within an organization to conduct computer intrusions. Their existing access and knowledge of the computer network makes it easier to cause damage to or steal data from the system.[73] Insiders are often involved in criminal activity for profit, whether directly through embezzlement or indirectly by passing information to criminal groups. For example, in 2001, two accountants working for Cisco Systems used their access to company computer systems to "illegally issue almost $8 million in Cisco stock to themselves."[74] Insiders, even if recruited by a foreign intelligence service to conduct espionage, fall into the criminal category.

Like hacktivists, terrorists are also individuals or groups who conduct politically motivated computer intrusions. The main difference, however, is the terrorist intent for violence. United States law defines terrorism as "premeditated, politically motivated violence perpetrated against noncombatant targets by sub-national groups or clandestine agents."[75] As previously discussed, since international laws, treaties, and conventions generally only recognize states, terrorists normally fall into the criminal category unless a specific UN resolution has sanctioned military operations against a terrorist group.

Cyber-terrorism is "the use of computers as weapons, or as targets" by terrorists.[76] Terrorists use the Internet extensively, but to this point "not for offensive actions."[77] Most computer intrusions by terrorists fall in the realm of CNE intended to gather information for potential

future lethal attacks. To date, there has been no published linkage of a CNA to a terrorist group.[78] In general, it would be very difficult to label a CNA as cyber-terrorism because of the difficulty in determining attribution and intent.[79]

General Alexander does not see terrorist groups as a major CNA threat currently, but that could change.[80] Nations on the DoS list of states that sponsor terrorism generated less than 1% of all reported computer intrusions in 2002.[81] Al Qaeda has used the Internet extensively to network its strategic communications with other terrorist groups and recruit disciples. Furthermore, Al Qaeda computers captured in Afghanistan had extensive data on dam controls and methods to potentially cause catastrophic failure of infrastructure control systems, showing planning and intent for future terrorist attacks.[82] Although terrorist groups might not have extensive CNA capabilities currently, they could obtain the required expertise in several ways: sending true believers to cyberspace schooling; trying to convert hackers to their cause; or paying criminal groups or hackers to execute their attacks by proxy.[83] By coordinating a proxy CNA with a physical terrorist attack, terrorist groups could feasibly degrade a state's ability to respond.[84]

Implications for the Intelligence Community

Leaders, policymakers, and other stakeholders must make many complex decisions regarding cyberspace. This section will highlight two that evolve from the preceding analysis of cyber law and sources of threats. First, they must decide what level of risk is acceptable in cyber security based on the threat. Second, they must determine how to respond to CNE and CNA. A key role of the intelligence community is to facilitate these decisions.

Having examined existing law, the sources of threats, and their status under law, what are the implications for the intelligence community in fulfilling this role? This paper proposes five imperatives that evolve from the previous analysis and which are important for the intelligence community to internalize in order to support these key decisions.

Imperative 1: Embed legal advisors. Legal advisors must be embedded in intelligence organizations undertaking computer network operations.

As previously stated, computer intrusions often fall into a gray area between crime and war requiring a case by case legal analysis using law by analogy. Intelligence organizations conducting cyberspace activities need lawyers for several purposes.

First, the lawyers can assist with legal determinations on which computer intrusions meet the threshold for an armed attack. These computer intrusions will generally fall under the purview of DoD or the CIA who make recommendations to the president and then execute appropriate foreign intelligence collection, covert action, or military responses. Computer intrusions that do not meet the armed attack threshold may be passed to the DoJ, DHS, or other domestic stakeholders for action if they qualify as crimes or relate to domestic terrorism or security concerns.

Second, legal expertise on intelligence law is necessary to ensure intelligence agencies are operating legally within their established authorities. For example, DoD intelligence agencies have limitations on the collection, retention, and dissemination of information on US persons as established by U.S. Code Title 50 Chapter 36, Executive Order 12333, and DoD Directive 5240.1-R. Agencies with domestic intelligence authorities have corresponding restrictions on foreign intelligence collection, retention, and dissemination. Additional limitations on authorities and collection methods exist in various other domestic intelligence laws and policies. These include the Foreign Intelligence Surveillance Act, Electronic Communication Privacy Act, the Patriot Act, Stored Communication Act, and Economic Espionage Act.[85]

Third, any organization that will conduct CNA will require legal expertise on the Laws of Armed Conflict (LOAC) to understand how the principles of military necessity, unnecessary suffering, proportionality and discrimination of military targets from civilian sites apply in cyberspace.[86] In the opening scenario, USCYBERCOM would require a legal determination of an armed attack based on attribution and intent in order to respond. The appropriate response would be tested against the LOAC.

Imperative 2: Quantify threat capabilities, intent, and vulnerabilities. The intelligence community must clearly quantify threat capabilities, intent, and vulnerabilities to facilitate the decisions of key stakeholders. One of the mission objectives of the U.S. National Intelligence Strategy (NIS) is to "enhance cybersecurity."[87] The NIS further emphasizes that one of the ways the intelligence community does this is "by expanding our knowledge of the capabilities, intentions, and cyber vulnerabilities of our adversaries."[88]

As stated above, stakeholders must decide what level of risk is acceptable in cyber security based on the threat. In order to do this, they must understand the threat's capabilities and intent. The United States has a diverse set of networks that vary from separate and secure classified DoD networks to Internet-based, privately-owned, critical infrastructure networks. Understanding the threat's cyberspace capabilities against the various networks in the United States and their intent for using those capabilities helps guide stakeholders' decisions about network security measures and federal regulations required to protect the nation's critical infrastructure.

The United States may be able to partner with nations or groups that possess cyberspace capabilities but no harmful intent in order to establish international norms and standards for cyber security. Limited resources and security measures are necessary to defend against threats with harmful intent but no cyberspace capabilities. In this case, the United States can focus its intelligence to ensure the threat does not partner with another to gain cyberspace capabilities to match its intent.

For example, in the opening scenario the United States should have focused its intelligence collection on any attempts by Iran to gain CNA capabilities. A threat that possesses both intent and capability requires the highest security measures, federal regulation, and priority intelligence monitoring.

In deciding how to respond to a computer intrusion, intelligence can provide decision makers with a better understanding of the threat's intent and vulnerability. Understanding the threat's intent (i.e., CNE versus CNA) makes a difference in the U.S. response. If the United States decides to respond in kind, understanding the adversary's

cyberspace vulnerability becomes important. A comprehensive CNA on U.S. infrastructure would require extensive planning and preparation.[89] This amount of preparation, surveillance, and testing is vulnerable to detection if intelligence is sufficiently focused and persistent in determining capabilities and intent.

As previously stated, determining attribution is very difficult. However, attribution is precisely what decision makers need from intelligence for both prevention and response. The NIS emphasizes that the intelligence community further enhances cyber security "by increasing our ability to detect and attribute adversary cyber activities."[90] Decision makers need attribution for suspicious computer intrusions and CNE to proactively determine the true nature of the threat, defend networks, and prevent potential escalation to CNA. Decision makers also need attribution for CNA to determine the status of the threat and attack under law and the appropriate response. In the opening scenario, USCYBERCOM could have made a recommendation on the appropriate response if attribution of the CNA was clear.

Imperative 3: Network analysis. This problem of attribution contributes to the third intelligence imperative, which is that network analysis is important in order to determine the true source of the threat. While certain members of the intelligence community have made great progress in using network analysis methods, progress is sporadic across the community as a whole.[91] The intelligence community, whether associated with military or law enforcement organizations, should be investing in data mining and link analysis technologies and training. Data mining is generally used to determine anomalies while link analysis finds commonalities.[92] These network analysis technologies can exploit large amounts of data and have proven to be powerful tools in determining affiliations and linkages while also highlighting the absence of linkages. For example, scientists at the Massachusetts Institute of Technology conducted an experiment in which they were able "to use network analysis to determine the sexual orientation of Facebook users even though these users had not disclosed their preferences publicly."[93]

Hackers conducting computer intrusions have social networks that can be charted and analyzed to effectively determine their linkages. The linkages could turn up associations with other hackers, hactivists,

and insiders; or in some cases criminal groups, terrorists, or foreign government agents directing the activity. For example, in the opening scenario, NSA successfully employed network analysis to determine Iranian government and Russian hacker associations. An absence of key linkages is also important because it can indicate an individual is less of a threat and not directed by criminal groups, terrorists, or a foreign nation.

Intelligence analysts can focus on key indicators that can be tracked through network analysis. As previously noted, terrorist groups are making extensive use of the Internet for strategic communications and recruiting but appear to have limited CNA expertise. There are a limited number of hackers with high-level expertise. Monitoring the social networks and movement of these individuals can indicate when a foreign nation, terrorist or criminal group is recruiting a hacker for training, preparation, or an actual attack.[94] For example, in the opening scenario, the HUMINT report on the Russian hacker's travels should have triggered additional intelligence collection to confirm the hacker's activities in Iran. Studies have shown that terrorist and criminal groups share technology and expertise for reasons more related to profit and gaining operational capability than ideological similarities.[95] Analysts can monitor hacker and terrorist chat rooms and web sites to determine linkages between the two and their potential sharing of technology and expertise.[96]

Imperative 4: All-source approach. An all-source approach to intelligence collection is necessary. This is directly tied into the problem of attribution and network analysis. Because cyberspace resides in the signals intelligence (SIGINT) discipline, it would be very easy to look at this solely as a SIGINT problem. However, telephony and computers do not have all the answers. Individuals with expertise in computer intrusions also generally have expertise conducting those intrusions in a way that electronically attributes the intrusions to another individual's computer using botnets. Thus, it would be very easy to make a false attribution using single-source SIGINT. Bringing other intelligence disciplines into the analysis should help capture such inconsistencies, as well as possibly show linkages not seen through SIGINT. In fact, the NIS specifically emphasizes the need to integrate CI with cyberspace to

protect critical infrastructure.[97] All intelligence disciplines can be used for collection on both foreign and domestic threats. The collection must be performed by the intelligence agencies with the correct foreign or domestic collection authorities under legal advice as discussed in the first intelligence imperative.

An all-source approach complicates the technology aspect of network analysis because HUMINT, imagery intelligence (IMINT), and CI come in various information formats that differ significantly from SIGINT. Data mining and link analysis technologies generally have limitations in handling non-structured formats that combine different types of information, like text and video. However, there have been significant advances in tagging these formats for data mining, and the intelligence community needs to continue to develop this capability in order to provide more comprehensive network analysis. In the opening scenario, better tagging of HUMINT may have allowed for its integration with SIGINT during network analysis to connect the dots on the Russian hacker-Iran connection.

Imperative 5: Improved intelligence sharing. Intelligence sharing must be improved both within the intelligence community and with key stakeholders. Having just highlighted the importance of a comprehensive all-source intelligence approach, it is crucial to share intelligence between the multiple stakeholders involved in order to improve detection and attribution. Additionally, intelligence sharing is especially important to place domestic and foreign intelligence into the hands of those intelligence agencies and stakeholders who have the legal authority to analyze and exercise proper response to a criminal act or act of war, as noted in the first imperative. The opening scenario highlighted problems with information sharing since the CIA's assessment of Iran as having intent with no capability was not informed by the SIGINT from NSA and HUMINT from DoS. The NIS recognizes this imperative with enterprise objectives to "strengthen partnerships" and "improve information integration and sharing."[98] According to the Comprehensive National Cybersecurity Initiative (CNCI), ODNI has responsibility to "connect current cyber centers to enhance cyber situational awareness and lead to greater integration and understanding of the cyber threat."[99]

Activities like the Cyber Storm series of exercises conducted by DHS have improved intelligence sharing with 13 countries, 11 states, and seven cabinet-level federal agencies which participated in the latest Cyber Storm III exercise.[100] However, there is still room for improvement. The exercise report from the Cyber Storm III exercise specifically cited that "exchanging and sharing classified information among organizations proved to be a challenge."[101]

Conclusion

The issues of cyberspace law are complex and unlikely to be resolved any time soon. Although efforts like the CoECC and UN WGIG represent progress in international cooperation on the development of cyberspace standards and norms, most of this progress is in the area of defining cyber-crime rather than cyber-war. Given U.S. interests in protecting privacy rights, the issues related to attribution will also endure. However, stakeholders require timely and accurate intelligence in order to make decisions on the legal status of a computer intrusion and its source as well as the appropriate response, whether criminal prosecution or military action.

Although the five intelligence imperatives proposed in this paper are not panaceas, they would greatly reduce the risk of the opening scenario ever happening in the United States. Applying these intelligence imperatives facilitates decisions and mitigates risk. Comprehensive network analysis and using an all-source intelligence analytical approach would assist with quantifying threat capabilities and intentions, thereby facilitating detection, prevention, attribution, and decision making. Increased intelligence sharing supports the all-source approach, facilitates collaboration between law enforcement and the military, and provides a common operating picture to all stakeholders. Finally, embedding experienced legal advisors into intelligence organizations involved in cyberspace activities will facilitate more timely determinations of legal status and appropriate responses by the agencies with the proper legal authorities.


U.S. ARMY WAR COLLEGE
Prudens
Futuri
Carlisle Barracks, PA

Section Two

Information Effects in the Cognitive Dimension


U.S. ARMY WAR COLLEGE
Prudens
Futuri
Carlisle Barracks, PA

Introduction

This section focuses on information effects in the cognitive dimension of the information environment designed to influence an intended audience's perceptions and attitudes, ultimately leading to a change in behavior. The Department of Defense (DoD) recognizes the importance of strategic communication and information operations in enabling mission success in this regard. Interestingly, theses concepts have evolved in fits and starts over the last decade as evidenced by a recent change in the definition of information operations and the recent completion of a DoD assessment study on strategic communication. The papers in this section examine several aspects of current information efforts and offers recommendations for improvement, thus contributing to clarifying both the overarching concepts and their associated challenges and opportunities.

Lieutenant Colonel Christopher Rate leads off with his essay titled, "Can't Count It, Can't Change It: Assessing Influence Operations Effectiveness." He examines what is arguably the Achilles heel of information operations and strategic communication, i.e. measuring the effectiveness of influencing the attitudes and behaviors of intended audiences. Colonel Rate recommends three requirements for improving cognitive assessments: 1) a comprehensive understanding of effectiveness measures, 2) the integration of evaluators at the beginning and throughout the planning process, and 3) the development of a cadre of personnel with the knowledge, skills and abilities to conduct assessments. In the end, effective assessments are essential to ensuring that influence operations will be an integral and credible part of any military operation.

In his paper, "Strategic Communication: The Meaning is in the People," Colonel David Johnson posits that senior leaders must embrace the communication process before they can effectively develop and implement a successful strategic communication plan. He emphasizes that the meaning of a message is *in the people* and not in the message itself. Colonel Johnson proposes a number of recommendations to facilitate a leader's understanding of and role in conducting strategic

communication as a critical skill set. These recommendations include changing the mindset of how leaders view the communication process as well as changing how they actually communicate. As with any plan, defining clear and actionable strategic communication objectives is key to success.

Together, the perceptive observations and careful analyses in these papers provide valuable insight into the cognitive dimension of the information environment as well as issues surrounding the information element of national power as it is applied in today's world.

Can't Count It, Can't Change It: Assessing Influence Operations Effectiveness

Lieutenant Colonel Christopher R. Rate
United States Air Force

For all persuasion artists who count with their hearts, souls, and guts, I only suggest counting like this: 1 = Yes the Other Guy Changed or 0 = No the Other Guy Did Not Change. And, if you cannot tell when, whether, or if the Other Guy changed, then persuasion is useless because persuasion is only about change.

—Dr. Steve Booth-Butterfield[1]

The battle for "hearts and minds" wages throughout the global information environment. For example, the favorable attitudes of Afghans towards the United States and its forces are declining. Although the Taliban, along with al Qaeda, receive the majority of the blame for the persistent violence in Afghanistan, they continue to propagate their message that the United States is attacking the religious faith of the Afghan nation.[2] Their ability to garner support of the Afghan population and to promote hatred toward any United States effort in Afghanistan has proven a challenge for influence operations practitioners. Yet, practitioners have asserted that the United States is "able to reach the people through leaflets, food, broadcast coordination, use of coalition forces, and good deeds to prove [the United States is] not attacking their religious faith … [and these] efforts have paid off and proven to be an effective measure in … efforts against terrorism."[3] Where is the evidence that these efforts are effective? How can the practitioners "prove" it?

The effectiveness of strategic influence operations is often the subject of considerable debate, simultaneously coming under fire by skeptics of the general effectiveness of influence operations, and by those who would provide direction and resources for influence activities. Influence practitioners generally understand that assessing the effectiveness of influence operations is part of the "process," but they lack the requisite

capabilities to accomplish it. It is, therefore, an imperative to fill this void as the future of strategic influence operations is inescapably dependent upon practitioners' abilities to objectively demonstrate its utility and success in influencing the attitudes and behaviors of intended audiences. Unfortunately, as of today, most members of the influence community do not get it. While this paper does not assert the merits of strategic influence operations, it certainly attempts to mitigate the knowledge vacuum and draw attention to several factors essential to assuring the greatest probability of success in assessing its effectiveness. These factors include a comprehensive understanding of effectiveness measures, the inclusion of campaign evaluators at the beginning and throughout the planning process, and the development of a cadre of personnel with the knowledge, skills and abilities to conduct assessments. Strategic influence operations are about changing attitudes and ultimately behaviors…but, if you "can't count it, you can't change it." And, this applies not only to foreign audiences but equally to the perceptions of influence operations skeptics.

What Does It Mean to Influence?

In order to proceed with a discussion on strategic influence operations, it is important to establish a common framework from which to work. Lexical definitions generally agree that "to influence" is to sway somebody, or to have an effect on somebody that helps to determine that person's actions, behavior, or way of thinking.[4] Similarly, in a military context, as defined by the Air Force Doctrine Document 2-5,

> ***Influence operations*** *[emphasis added] are focused on affecting the perceptions and behaviors of leaders, groups, or entire populations. Influence operations employ capabilities to affect behaviors, protect operations, communicate commander's intent, and project accurate information to achieve desired effects across the cognitive domain.*[5]

Related to influence operations are the concepts of strategic communication (SC), psychological operations (PSYOP; now referred to as military information support operations (MISO)), and information operations (IO). Although their definitions are not entirely distinct (see Table 1), the concepts clearly overlap in their endeavor to affect the cognitive dimension of the information environment.

Therefore, influence operations (IFO) will be used in a generic sense, when appropriate, to describe activities to influence the attitudes, opinions, and ultimately behaviors of targeted foreign audiences.

Term	Definition
Influence Operations	Influence operations are focused on affecting the perceptions and behaviors of leaders, groups, or entire populations. Influence operations employ capabilities to affect behaviors, protect operations, communicate commander's intent, and project accurate information to achieve desired effects across the cognitive domain.[6]
Information Operations	The integrated employment of the core capabilities of electronic warfare, computer network operations, psychological operations, military deception, and operations security, in concert with specified supporting and related capabilities to influence, disrupt, corrupt, or usurp adversarial human and automated decision-making, while protecting our own.[7]
Psychological Operations (PSYOP, aka Military Information Support Operations)	Planned operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately behavior of foreign governments, organizations, groups, and individuals. The purpose of PSYOP is to induce or reinforce foreign attitudes and behavior favorable to the originator's objectives.[8]
Strategic Communication	Focused United States Government efforts to understand and engage key audiences to create, strengthen, or preserve conditions favorable for the advancement of United States Government interests, policies, and objectives through the use of coordinated programs, plans, themes, messages, and products synchronized with the actions of all instruments of national power.[9]

Table 1: U.S. Military Doctrinal Definitions—Influencing the Cognitive Dimension

In addition to strategic influence operations, it is important to understand the dimension of the information environment that is intended to be affected, that is, the *cognitive dimension*. The cognitive dimension—which, as it implies, exists in the human mind—includes the desired perceptions and attitudes of the intended populations of interest.[10] Humans process information they receive within this cognitive dimension. The information is filtered through an individual's unique experiences and biases (perceptions, opinions, attitudes, and beliefs) that act to provide a sense of meaning and context to the information.[11] Because words matter, establishing a common vernacular is an important first step in understanding influence operations. In the end, however, the influence practitioner must understand the effect of influence operations on the cognitive dimension of the audience. Without this knowledge, it is impossible for the influence practitioner to champion, judge, or even defend the effectiveness of the influence activities. The ability of the practitioner to demonstrate the utility of influence operations is critical toward influencing the perceptions of a key audience; that is, influence operations skeptics.

Audience Analysis: The Skeptics

"We have met the enemy and he is us."[12] Fueled by an inability of the influence community at large to articulate the utility of their art, several key audiences have expressed strong skepticism of strategic influence operations. Representative of this accelerant, an influence operator confessed, "I have a huge problem explaining…what we do. For too long the 'lead-down-range' leaders have decided that since [they] don't understand IO, PSYOPs [sic], or any other non-kinetic capability, they will simply choose to ignore it."[13] The absence of or lack of immediacy of results often leads military commanders to question the value of influence operations.[14] It is often the fact that commanders are steeped in this culture of kinetic operations, but "the commander also needs to overcome the false need for instant gratification that is the expected norm for kinetic measures of effectiveness [MOE]."[15] Explicably, a significant contributor to this quandary is the lack of a complete story to tell by the influence community. "Doing stuff" doesn't sell well without the "so what." Quickly seizing this fact one skeptic caustically derided,

> *Perhaps the greatest psychological operation (PSYOP) campaign is the one in which the PSYOP community has exalted the effectiveness of their trade as a combat multiplier and peacetime contributor in the pursuit of national and military objectives. Members of the PSYOP community oftentimes present a slightly one-sided portrayal of PSYOPS [sic] as "an extremely imaginative and versatile force multiplier" despite undisclosed shortcomings manifested in an inadequate system of assessment.*[16]

In addition to the skepticism described above, there has been an emerging concern regarding influence operations at the highest levels of government. In July 2009, the late Congressman John Murtha, then chairman of the House Appropriations Defense Subcommittee cut out more than half of President Obama's fiscal year 2010 budget for military influence operations. According to the House Appropriations Committee report:

> *[President Obama's] budget request includes nearly one billion dollars for Department of Defense information operations (IO) programs. The Committee has serious concerns about…the significant amount of funding being spent on these programs.... The Committee questions the effectiveness of much of the material being produced with this funding, the supposed efforts to minimize target audience knowledge of United States Governmental sponsorship of certain production materials, and the ability of the Department to* ***evaluate the impact of these programs*** *[emphasis added].*[17]

From the perspective of Congress, the Department of Defense was spending vast amounts of money on influence operations. These activities tended to be conducted in secrecy and their effectiveness could not be measured.[18] Congress' ever-increasing frustration with the Defense Department's initial billion dollar request led appropriators to press the Defense Department on its influence operations requirements. When pushed, the Defense Department reduced its request to $626 million. Unsatisfied, Congressional defense appropriators then slashed another $100 million off the request. It was the opinion of Congress that the Department of Defense did not know what its influence operations "needs were, what they had, and what they should cost."[19] Now that Congressional oversight is tightening, Congress

has directed the Department of Defense to consolidate its influence operations requirements in one place. Under increasing scrutiny, future appropriations may certainly be tied to a demonstrated return on investment. In fact, an independent analysis of Defense influence operations activities has arrived at several similar conclusions, that: (a) Congress should tighten its oversight of influence operations; (b) the Department of Defense should conduct a full audit of its influence programs and projects; and (c) the Department of Defense should develop metrics to gauge the effectiveness of their influence programs.[20] Clearly, the influence practitioners have failed to articulate the importance of influence operations and have been unable to persuade the highest echelons of government of its effectiveness. Again, if you don't have a complete story, it becomes a moot story to tell.

In what appears to be an acknowledgement to the United States Congress that assessments of influence operations are lacking, President Obama reported that "it is important to the effectiveness of our programs that we develop the capacity to measure success and emphasize accountability."[21] If the skeptics have not made it plainly, if not painfully evident, the common denominator at the foundation of the criticisms and critiques is the absence of measures of effectiveness and deliberate campaign evaluation planning. These perceptions cannot easily be discounted. Perceptions are at the heart of the influence business, and therefore influence practitioners must not only influence their foreign target audiences, but they must also be able to influence the perceptions of their skeptics and resource providers. To accomplish this feat, the influence community must have an understanding of the complexities surrounding the assessment of influence operations. The bottom line is that "if you can't count it, you can't change it."

Towards an Understanding of MOE

Evaluation Types. Assessing the effectiveness of influence operations, "counting it," is a challenging proposition. Influence operations are growing more sophisticated and strategic, and the evaluation component is not keeping pace with the innovation of influence practitioners. Further, there is typically a misperception of what information can be provided back to a campaign by the various types of evaluations

during the campaign process. A description of the three major types of evaluations follows:

- Formative evaluation: The formative evaluation assesses the strengths and weaknesses of campaign products and strategies before or during the campaign's execution; identifies beliefs, attitudes, behavior, etc. of target audiences; defines environmental conditions; establishes *baselines metrics*.[22]
- Process evaluation – measures of performance (MOP): MOPs are criteria used to assess friendly actions that are tied to measuring task accomplishment.[23] An MOP assesses whether influence practitioners are "doing things right" and how well the influence activities involved are working (e.g., distribution of materials, campaign reach, how many people reached, etc.).
- Outcome/impact evaluation – measure of effectiveness (MOE): MOEs are criteria used to assess changes in system behavior, capability, or operational environment that is tied to measuring the attainment of an end state, achievement of an objective, or creation of an effect.[24] An MOE assesses whether influence practitioners are "doing the right things" and whether the influence activities involved are contributing to the attainment of outcomes and objectives (e.g., changes in attitudes and behaviors) in the intended audiences.[25]

Subsequent to the establishment of baseline audience attitudinal and behavioral metrics, arguably the most important evaluation type is the outcome evaluation, that is, the MOE. Unfortunately, even with an unambiguous explanation of the measures, there is often confusion between the concepts. At times, MOPs are misused to portray campaign effectiveness and the obtainment of objectives. For example, consider an influence campaign using the internet as the medium to deliver an influence message to a specific target audience to attain an attitudinal or behavioral objective. Influence practitioners may point to the number of "hits" on the website as a measure of campaign success. In fact, this is not a measure of effectiveness; rather, it is an MOP assessing that the campaign is reaching some audience (whether the specified target audience is being reached is a separate question). This example highlights how there was no linkage between the collection

and a stated, measurable objective – what attitudes, opinions, behaviors were assessed that would determine if the campaign was having an effect. Some practitioners, desperate to present some level of campaign success, rely on such measures (MOPs) that though important, do not capture the outcomes or effects (MOEs) of the campaign, and are in no way meaningful from an impact or outcome point of view.[26] It is simply that without MOEs, "some campaigns try to dazzle with a long list of process measures, or measures of their implementation and effort."[27] MOPs will never suffice or replace MOEs in determining the attainment of objectives.

Another source of confusion regarding what information can be derived from evaluation measures comes from the *Commander's Handbook for Strategic Communication and Communication Strategy,* which makes the highly equivocal statement that future influence operations outcomes can be predicted based on assessment results.[28] This is a misuse of these evaluations, MOEs and MOPs, which are intentionally designed to be descriptive; that is, these measures inform the practitioner of "what is," not necessarily "what will be." An additional word of caution to influence practitioners regarding the misuse of evaluations is that MOEs do not equate to influence operations success. Though MOEs may show progress towards accomplishing an objective, it is quite possible to interpret MOE data that indicates the influence campaign is having no or detrimental effects. When this information is fed back into the campaign, the influence practitioner must decide whether to stay or adjust the course of the campaign, or cease activities altogether. Influence operations are inherently iterative and must remain flexible to respond to the changing information environment as indicated by the assessments results.

Attitudes versus Behaviors. B.H. Liddell Hart said, "to influence man's thought is far more important and more lasting in effect than to control their bodies or regulate their actions…."[29] During the development of MOEs, influence practitioners will soon come to the realization that human behavior is complex, and that trying to influence human behavior is difficult. It is, however, myopic to focus only on influencing behavior. MOEs *are not* all about behavior. Those who hold this view sell influence operations short of its full potential.[30]

This naïve approach to MOE development could signal frustration for the influence arena as it ignores potential short, intermediate, and long-term effects that may suggest that the influence campaign is impacting the target audience towards a desired condition.

Most external influences (e.g., media) do not shape behavior directly, but affect change through processes in the cognitive domain of the information environment. Though one might agree that behavioral change is our ultimate goal, often it is not necessary or even plausible to measure behavior, especially if the behavior of interest is unobservable. According to Icek Ajzen, "we generally seem to behave in ways that are consistent with our attitudes."[31] Therefore, attempting to influence a change in behavior without first influencing attitudes, values, or beliefs is not sustainable without the continual presence of the influence activity. Without attitudinal change, the audience will return to its original or previous behavior once the influence activity is terminated.

Causation: Can it be proved? Adding to the complexity of assessment measures is the question of whether observed changes in attitudes and behavior can be directly attributed to any specific influence activity. Cause-effect questions continually arise during the evaluation of influence operations. Knowing the effects, if any, a program has is critical for assessing the program's merits or worth.[32] Cause-effect assessments of human emotions, motives, objective reasoning, and behaviors of organizations, groups or individuals are simply no easy task, often requiring specialized education in this domain in addition to knowledge of research design and evaluation. Further, as a condition of the operational environment or an inability to collect sufficient data, determining causality may be unfeasible. This leaves the influence practitioner with only a confirmation that influence activities may somehow be associated to a change in audience attitudes or behaviors. Is this sufficient?[33] Assessments in general should not be approached in this manner. Determining the strength of association versus a cause-effect relationship between two variables – the influence activity and change in attitude/behavior – is limited by data collection methods. Due to this, the influence practitioner should strive for the more rigorous approaches to assessing influence operations effectiveness. Through careful, deliberate planning of assessments and data collection

methods, causal inferences can be made with increased confidence allowing practitioners to sell the "rest of the story" to the skeptics of influence operations.

As previously mentioned, one's ability to make causal inferences is a function of how one collects data. Causal inferences must be made through experimental (or quasi-experimental) means, accounting for unrelated variables which might confound the results, that is, factors that could suggest alternative, competing explanations for changes in attitudes and behaviors. Having gathered the data in this fashion, one should be more comfortable in making a causal inference. For example, individuals from the intended audience are first randomly assigned to either an influence or control group, and data is collected for both groups establishing a baseline. Following exposure to the influence activity, data is collected for the influence group. At the same time, data is again collected for the control group that was not exposed to the influence activity. Once the extraneous factors have been eliminated, accounted for, or controlled, then causal inferences may be drawn from the analysis of the data. But again, causality depends on the data collection methodology. Unfortunately, most designs employed in influence operations today are simply single group post-test observations or designs that measure a single group before and after it has received the stimulus. In each case, any attempt to infer causation is equivocal. Since there is no control (or comparison group) in addition to a host of possible factors that may have influenced changes in attitudes and behaviors between the pre- and post-test observations, there is no way to account for alternative explanations for the assessment results.[34] It is important to reiterate that careful, deliberate assessment designs can be employed to better approximate the cause-effect relationship sought in influence operations.

Campaign Evaluation: A Mitigation Plan

As reminder, this paper is not arguing whether influence operations are effective, rather its focus is about bringing to light the challenges to influence operations from key skeptics; and, it attempts to clarify some misperceptions surrounding the assessment of influence operations effectiveness. As previously described, it is important to understand

the perceptions of the skeptics and some critical misunderstandings surrounding the assessment of influence operations effectiveness. Armed with this knowledge, a mitigation plan can be designed to help influence practitioners articulate a full and accurate story of the utility of influence operations.

Inherently, most campaign models follow a logical process. The process models operate on what to do and in what sequence, allowing the influence practitioner some flexibility to be creative, but leaves ambiguity in how what they do to impact social behaviors. Practitioners are very adept at following their processes, but few have an adequate in-depth understanding of "why" they are doing certain steps or phases. There is an art and science to this process. The practitioners employ the art, but there is a lack of science which could ultimately enable them to do their jobs more effectively. Influence operations is the confluence of art and science, it takes a richer understanding of the science to produce the better art, thereby creating a greater probability of developing an intervention that will in the end be effective.

Theoretical Underpinnings. In order to change behavior, influence practitioners should possess a rudimentary understanding of why people behave and think the way they do, while evaluators must possess an in-depth knowledge. Several theoretical models of human attitudinal and behavior change can provide this foundation, with one of the most prevalent and applicable to influence operations being the Theory of Planned Behavior (TPB). TPB is one of the most studied and applied psychological theories of motivation and behavior, being applied to myriad studies ranging from health behavior to business ethics.

The model (as depicted in Figure 1, following page) suggests that human behavior is primarily determined by the intention to perform a particular behavior. Working backwards, three major factors influence those behavioral intentions: an individual's attitudes toward the behavior, an individual's belief that others important to the individual have expectations of his or her performance of the behavior, and the individual's belief in his or her ability to perform the behavior. These factors are then influenced, respectively, by an individual's beliefs about the likely consequence of the behavior, an individual's beliefs regarding social norms, and an individual's beliefs about the presence of factors

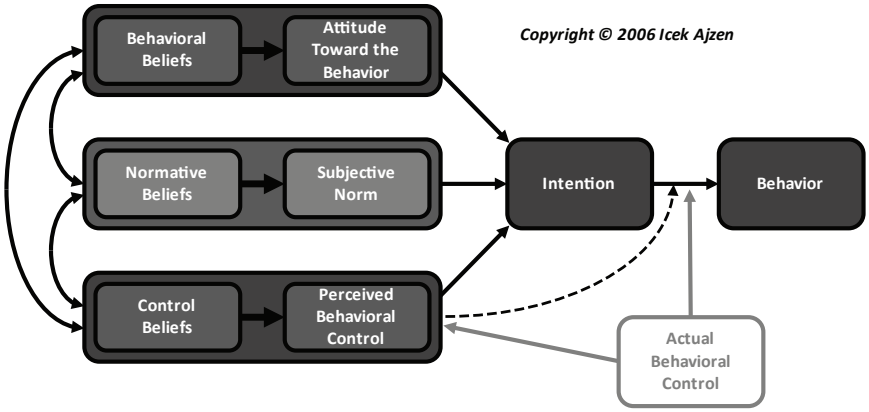

Figure 1: Icek Ajzen's Theory of Planned Behavior Model[35]

that may facilitate or impede performance of the behavior.[36] A strong comprehension of this model not only allows the influence practitioner to design influence activities to achieve desired effects across the cognitive domain, but also allows the development of short, intermediate, and long term MOEs focused on changes in target audience attitudes, norms, perceptions, and behavioral intentions in order to ultimately influence changes in behavior. In reference to a similar model, Dr. Anthony Pratkanis stated, "I like this approach a lot because it forces one to think about each objective of the communication and whether or not that objective is important for the overall mission. It gets away from thinking of leaflets (or whatever) as magic bullets that magically get people to magically do stuff."[37] To reiterate, "a deep understanding of the human behavior model…is critical to obtaining behavior change that is driven by perceptions and attitude, thus ensuring the desired information end-state."[38]

Good Evaluation Starts at the Beginning. Currently, assessment of MOEs is largely an ad hoc ability. Although the attention paid to MOEs in joint doctrine is negligible, some doctrine clearly is instructive that good campaign evaluation planning starts at the beginning of the influence operations planning process. From the beginning stages, "the social and behavioral sciences…provide insight as to what PSYOP soldiers should take into consideration when planning and conducting

PSYOP."[39] The challenge inherent within this statement is rather complex. Understanding the human condition and how to persuade or influence attitudes and behaviors through an appropriate medium is a daunting task even for even the most experienced influence practitioner or social science influence expert. Effective employment of influence necessitates optimizing the art and science. Together, the practitioner and social science expert can bring multiple perspectives to bear with the goal of finding a common solution to meet the objectives of planned influence operations. The more we know and understand about the science, the better art we can produce. This deliberate blending introduces both challenges and opportunities for influence operations to showcase its utility.[40] To ensure a successful development of an evaluation plan, the desired effects and the assessment measures of influence operations must be determined during the formative stages of the planning process.[41] In other words, the MOEs and MOPs are crafted at this time to ensure that the chosen effects, objectives, or conditions are measureable. It is often the case that objectives are chosen that are beyond the scope of influence operations or are simply not measureable as described by the desired effects (e.g., defining a desired effect as the absence of an attitude or behavior). If the chosen effect "can't be counted," then it "can't be changed," and therefore, it is not a valid MOE or MOP and must be reworked. This initial iterative process is essential to good campaign evaluation design.[42]

Just as science and art are integrated, the influence operations planning process must demand that influence practitioner and evaluator work hand-in-hand from the beginning of the process. This joint endeavor ensures that the overall objectives meet the commander's intent, while also ensuring that specific, measureable supporting objectives are developed to help shape assessment criteria. The influence evaluator consults with practitioners to develop well-defined supporting objectives that are quantifiable and lend themselves to gathering accurate and valid baseline data. Formulating well-defined objectives is an iterative and collaborative process that sets the stage for all subsequent steps in the process of planning influence operations and campaign assessment.

A typical example of a comprehensive assessment program facilitated by influence evaluators generally follows a 5-step logic methodology

to evaluate influence operations that includes: (1) defining objectives; (2) developing the research approach; (3) designing data collection instruments and plans, (4) implementing and validating the research strategy, and (5) evaluating the data and reporting the results.[43] Two conditions must be met in order to have confidence in the assessment program. First, the influence operations must have clearly stated, observable and measureable objectives. Second, there must be reasonable assurance that the intended target audience has received the stimulus being evaluated.[44]

During the evaluation planning process, which runs parallel to influence operations planning, the evaluator relies on an understanding of a theory of human behavior (e.g., Theory of Planned Behavior) to support the development of the main and secondary objectives. These objectives describe the desired conditions of target audience attitudes and behaviors. The evaluators use the objectives to drive assessment criteria while concurrently seeking input on the developing criteria from the influence practitioners, behavioral scientists, strategic intelligence analysts, and cultural advisors. The methods used to collect MOEs are then internally and externally tested, as appropriate, before execution in the field. Evaluators ensure the methods used to collect the data give the campaign practitioners the optimal chance of making causal inferences if supported by the data analysis and interpretation. After ensuring reasonable reliability and validity of the measures, the collection methods are executed by qualified personnel. Following data collection, the evaluator analyzes and interprets the data to determine if the progress is being made toward the attainment of the influence objectives, and whether causal inferences can be made linking the influence program to attitudinal and behavioral changes in the target audiences.

Influence and Assessment Specialists

Throughout this paper it has been noted that evaluating the effectiveness of influence operations is challenging and difficult. It is also commonly acknowledged that corresponding measurements are "costly in terms of time, money, and manpower and usually require special expertise."[45] To the latter point, a March 2010 report to Congress

from the Department of Defense noted that most analysis of influence operations was conducted by defense contractors due to the lack of requisite skills within the Department. However, the government and military officials retained the responsibility for setting the objectives, targets, and policies.[46] Exploiting this apparent lack of capability, major defense contractors, as well as start-ups with little or no history or expertise in influence operations began casting themselves as influence specialists.[47] Further, Influence operations contracts were being won by contracting organizations whose ranks were filled with the same personnel who did not have the requisite evaluation and analysis skills while they were in uniform. [48]

In what can be interpreted as a veiled capitulation that assessments are too difficult, too challenging, too complex, joint doctrine warns commanders:

> *When assessing operations, JFCs [joint force commanders] and staff's should avoid excessive analysis. Excessive time and energy spent developing elaborate assessment tools and graphs squanders resources better devoted to other elements of the operations process. Effective JFCs avoid overburdening subordinates and staffs with assessment and collection tasks beyond their capabilities.*[49]

Although there are factions who would take this admonishment as an opportunity to relegate MOEs to the shadows, others clearly envision this as an opportunity to develop a cadre of uniformed personnel capable of addressing the issue of measuring campaign effectiveness.

Most military members have only a minimal understanding of the human and cognitive dimensions of target audiences and even less understanding of how to assess changes in these dimensions. Beliefs that some influence practitioners tend to be more adept at understanding the nuances of segmented audience research and analysis is questionable;[50] however, in actuality, influence practitioners are ill-equipped for the task. The qualification training in influence operations prepares practitioners to follow a process but provides an inadequate understanding of the human condition and the complexities of campaign evaluation. "The fact remains that an intuitive understanding of or an advanced education in psychology, sociology, or cultural anthropology will not

broadly occur among America's warfighting commanders."[51] Again, this highlights the importance of developing a skilled cadre – a cadre that can provide the expertise to assess influence operations effectiveness and provide influence practitioners the "rest of the story" to persuade skeptics of the utility of influence operations.

The Behavioral Scientist/Evaluator. The creation of a cadre with the ability to assess changes in the cognitive dimension of the information environment is necessary to fill the current void. In efforts to supplement the core of Army influence practitioners, the Air Force has recently begun to create what it also believes is a cadre of influence specialists. It has outlined the requirements for the award of a special experience identifier to include the completion of two influence operations courses and an advanced degree in an academic discipline related to the execution and planning of influence operations.[52] In its desire to participate in influence operations, the Air Force is essentially duplicating an Army capability. The Air Force is simply increasing the pool of influence practitioners, not addressing the need for an *influence evaluation* cadre. The Air Force should be strongly encouraged to seize this opportunity to fill the specialized niche left void by the lack of uniformed influence evaluators, a function better enabling influence practitioners to conduct influence operations.

Ripe for development into the role of influence evaluator, the Air Force behavioral sciences career field conveys to influence operations a unique combination of social sciences expertise coupled with strong assessment skills. It is the critical and creative thinking processes, in-depth knowledge of the human dimension that are developed and engrained during the process of obtaining an advanced degree, along with the requisite assessment capabilities, that act as a niche force enabler to the existing influence practitioners, especially at the strategic level. Again, the goal should not be to duplicate, rather to enable influence practitioners to do their job better.

Arguably, the most significant contributions to the assessment of influence operations effectiveness have been made by a small cadre of uniform and civilian social and behavioral scientists at the Joint Military Information Support Command (JMISC), United States Special Operations Command, in Tampa, Florida. *In 2007, the JMSIC*

created this element, which included seven doctorate-level scientists with varying backgrounds (e.g., social-cognitive psychology, clinical psychology, educational psychology, sociology, social work, etc.) at its full complement. Collectively, they study all aspects of society – from past events and achievements to human behavior and relationships among groups – and investigate the decision processes and communication strategies within and between humans in a social system. They provide insights into the different ways individuals, groups, and institutions make decisions and affect relationships, exercise power, and respond to change. As influence operations enablers, the JMISC behavioral scientists are adept in the science of human influence and the methodologies to assess its change. This specialized cadre has developed a robust assessment capability that has been attempting to measure the effectiveness of influence operations where others have dared not even try. Since 2007, they have continually proven their skills, providing assessment assistance for influence operations throughout the Department of Defense and interagency. It is important to reemphasize that these assessment positions often require advanced, specialized academic education to provide effective support to influence operations. The advanced degrees not only bring an expert level of critical, strategic analysis, but also credibility while interacting with other Department of Defense components, the interagency, and academia.

Typically, JMISC behavioral scientists perform the role of consultant or adviser while ensuring the appropriate conduct, coordination, execution and integration of behavioral sciences into strategic influence operations research and application. The following section highlights the significant roles, primary and supporting, of the behavioral scientist as an enabler within the influence operations process:

- Develops initial overarching objectives and assessment criteria.
- Advises on the selection of target audiences.
- Provides a comprehensive background in understanding human behavior, persuasion and influence, along with the processes that lead to constructive behavior change.
- Facilitates defining conditions, vulnerabilities, lines of persuasion and MOEs.

- Provides supported theories of human behavior and analyzes relevant databases and psychosocial-cultural research.
- Provides audience segmentations according to similar patterns of attitudes, beliefs and opinions.
- Develops MOEs and impact indicators used to evaluate progress of the campaign toward achieving its objectives.
- Develops baseline measures used to establish the current objective-related attitudes and/or behaviors of the target audience.

In addition to the roles delineated above, the behavioral scientist is the linchpin to executing influence activities and evaluation. The behavioral scientist formulates and implements an evaluation plan to assess the impact of influence activities over time. The evaluation plan involves collecting multiple data points to compare against baseline assessments. This process aids in monitoring potential changes in the intended audience – changes related to the objectives – subsequent to the implementation of influence activities. The behavioral scientist consults on the sequencing and timing of assessments and then analyzes and interprets the collected data. Most importantly, the MOE data collected over time is used as constructive feedback to provide rationale for necessary adjustments to the campaign based on its impact on the audience.

In summary, the JMISC model should be the standard by which influence practitioners will be able to influence intended audiences. At the same time practitioners will be equipped to answer the questions raised by influence skeptics. When senior leaders in the Defense Department and Congress understand and are persuaded by a complete narrative of influence utility, they will have the confidence to advocate for influence activities knowing that their guidance and resources are being translated into effective operations. By integrating the expertise and support of behavioral scientists into the influence operations process and daily operations of the JMISC, the command has demonstrated that an optimal blend of "science" and "art" increases the prospects for success in the arena of strategic influence operations. This is not a process of "art" then "science," but a deliberate integration of the two throughout the entire process.

Conclusion

It is inevitable that in a time of shrinking defense budgets, skeptics of influence operations will continue to doubt its effectiveness and make concerted attempts to acquire its resources. However, it will not be the result of the influence practitioner being unable to justify and defend his profession. If the influence practitioner and evaluator join their efforts and expertise at the beginning and throughout the influence operations process, a narrative of influence utility can be propagated throughout the Department of Defense to those who wish to communicate its success, and to those in Congress who desire to receive this information. The "hard work" in assessing influence operations effectiveness will come with educating practitioners on the nuances and complexities of MOEs and its development, and mitigation efforts to ensure good evaluation starts at the beginning. The crucial component of all these recommendations is the creation of a specialized cadre with the requisite skill to assess influence operations effectiveness. Taking steps now to build an integrated team of practitioners and evaluators will ensure that, in the end, influence operations will be an essential, critical, and credible part of any military operation, supported by the necessary expertise required to effectively achieve military objectives.[53] By demonstrating the ability to measure the effectiveness of influence operations, the community can persuade skeptics that, in fact, influence operations are changing the attitudes and behaviors of target audiences. Because, in the end…when we can count it, we can change it!


U.S. ARMY WAR COLLEGE
Prudens
Futuri
Carlisle Barracks, PA

Strategic Communication: The Meaning is in the People

Colonel David G. Johnson
United States Army

No human capability has been more fundamental to the development of civilization than the ability to collect, share, and apply knowledge. Civilization has been possible only through the process of human communication.

—Fredrick Williams[1]

The speed at which communication travels through the global information environment facilitated by the Internet, social media and the traditional forms of the news media requires leaders to receive, understand, and decide, but also to act on this information if they are to influence to their advantage and achieve the desired outcome. Since its debut, the term strategic communication (SC) has become a mainstay in many senior leaders' vocabulary and the "catch all" for many things only remotely associated with communication. It has been analyzed, debated and criticized. It continues to be a subject that garners its fair share of attention in blogs, journals and academia, yet it is still generally misunderstood in both military and government organizations.

In some forums, SC is referred to, in the plural form, as strategic communications (emphasis added). In other forums, the term takes the singular form. Some defense experts view SC as an interactive process while others see it as a simple collection of capabilities such as public affairs, psychological operations, and public diplomacy. In military circles, it is often synonymous with media engagement or crafting and disseminating messages, much the same way marketing or advertising firms manage their public relations campaigns.[2] Finally, there are senior leaders, like Admiral Michael G. Mullen, Chairman of the Joint Chiefs of Staff, who view SC as a way of thinking.[3] This conversation taking place is healthy and important in order to gain

a better understanding and appreciation for coordinated, integrated, and synchronized communication within and outside the interagency. However, much of the dialogue continues to focus on what constitutes SC and what does not. The conversation needs to focus on the latter half of the term, communication, the core element of SC. The ability to influence perceptions and change behaviors will become increasingly important and challenging in future conflicts and crises. Leaders will need to make a substantial investment in their own cerebral appreciation, and apply as much concentration and effort to shaping the communication narrative as they would with planning and executing the next operation.[4]

Before embarking on an SC strategy to win the hearts and minds of a selected audience, leaders should ask themselves and those around them, what is communication and what does it entail? SC is less about being first with the truth or "bumper sticker" themes; it is more concerned with engaging in conversation, developing relationships and influencing behaviors. The Prussian military strategist Carl Von Clausewitz said, "Everything in war is very simple, but the simplest thing is difficult."[5] Replace "war" with "communication" and Clausewitz's statement has some truth to it. However, if communication is so simple or so fundamental to civilization, as Fredrick Williams asserts, why does it continue to be an area where leaders tend to miss the mark?

Admiral Mullen asserts in his 2009 *Joint Force Quarterly* article, "Strategic Communication: Getting Back to Basics," that leaders are not bad at communicating; they simply struggle with credibility and ensuring their actions match their words.[6] If we accept the view that credibility, actions and words are intertwined and fundamental to successful communication, one could infer that what the Admiral is implying is leaders do not communicate well at all. In his testimony on SC and public opinion before the House Committee on Foreign Affairs, J. Michael Waller, Ph.D., states that communication entails understanding that everything we say or do, or do not say or do, sends a message. He went as far to state that the problem with SC is simple; it is a matter of changing the way people think about communication.[7]

In his article, "Why General Petraeus is Better Suited for Our Afghanistan Mission than General McChrystal Ever Was," Steven

Metz, chairman of the Regional Strategy and Planning Department at the U.S. Army War College Strategic Studies Institute, asserts that leaders like General McChrystal are without question talented combat commanders, but when it comes to be a strategic communicator, they struggle with knowing how to communicate.[8] During Army Leader Day at the United States Army War College in October 2010, when asked to opine on the subject of SC, one general officer responded by stating that "Strategic communication is nothing more than communication."[9] In essence, this general officer was spot-on with his response. Actions, images and words communicate a message to a certain person, group or audience.

"Successful strategic communication requires an interactive relationship between senders and receivers."[10] SC, in essence, is all about communication, but do leaders embrace this view, and more importantly do they understand it? If leaders, military or civilian, corporate or government, don't understand the communication process, they cannot effectively develop and implement a successful SC plan or strategy for their organization. A change in the paradigm of how leaders view and understand the communication process is needed. It starts with getting back to basics as Admiral Mullen has declared; it is time leaders understand why and how to communicate in order to affect SC.

Overview of the Communication Process

> *Communication (human communication, at least) is something people do. To understand the human communication process one must understand how people relate to each.*[11]

The communication process is comprised of multiple, interrelated elements such as message transmission, social relationships, context surrounding the message or image, the symbolic nature attached to the message, the condition or conditions in which the message is received, the abilities of the receiver, and his inherent and cultured responses.[12] Communication scholar David Berlo posits that the underlying purpose of communication is to influence. Berlo contends that successful communication starts with the communicator knowing his desired intent as a result of his message. The communication process continues

with the sender of the communication not only discovering how his message affects or influences his environment, but how it affects the belief and behavior of the receiver.[13]

Communication is a reciprocal process of exchanging signals to inform, instruct, or persuade, based on shared meanings and conditioned by the communicators' relationship and the social context.[14] Communication is the bridge that connects people with one another. It involves people, groups, organizations and societies. It involves influencing each other and being informed. In order to understand the human communication process, one must understand how people relate to each other.[15] The 2008 Defense Science Board's Task Force's final report on SC identified five sustained activities in order for the Department of Defense to be successful. These included understanding, advising, engaging, influencing, and measuring. In all but the final activity, the communication process is apparent. For example, the act of engaging consists of a "dialogue of ideas between people and institutions that support national interests and, wherever possible, common interests and shared values."[16] The point here is that the communication process is an integral component and interwoven throughout SC. Without effective communication, SC cannot be sustained.

Recommendations

Change the Mindset.

The communication process has evolved over the past several decades from one that was message-centric to one that is audience based, complex, culturally dependent and meaning dominant.[17] Today, the communication narrative or message fails because it does not consider "the complexities of communication as a *meaning-making* process."[18] It is time to rethink what makes SC effective; it starts with changing the mindset of how leaders view and understand the communication process. The phrase "words have meaning" can probably be traced back to elementary or grade school. Today, it is the dominating paradigm at the U.S. Army War College, the Army's premier graduate-level institution for strategic leadership. Professors and students alike fail to understand that by saying "words have meaning" they ignore the

cognitive dimension of the person or group on the receiving end of the communication stream. Leaders, in the military or government, have to break away from this traditional communication thought process that words have meaning and adopt an understanding that words don't have meaning, people do.

> *Communication does not consist of the transmission of meaning. Meanings are not transmittable, not transferable. Only messages are transmittable, and meanings are not in the message, they are in the message-users.*[19]

Leaders must change from a "me" centric view of communication to a "we" focused view. It entails understanding that the meaning of any action, image or word is not in the sender, but in the hearts and minds of the person or group receiving the message.[20]

During U.S. Congressman Steve Cohen's remarks before Congress on January 18, 2011, he compared the Republican's tactics to repeal the health care law to those of the Nazis prior to the Holocaust. "They don't like the truth so they summarily dismiss it. They say it's a government takeover of health care, a big lie just like the (Nazi propagandist Joseph) Goebbels."[21] Many might contend that the Congressman demonstrated poor judgment in his selection of words. This might be true; however, this essay contends that the Congressman did not consider how his remarks would be interpreted in the hearts and minds of those not only sitting in the chamber, but by the news media and consequently the American audience. Congressman Cohen did not consider that his "messages are always interpreted within a larger, ongoing communication system."[22]

President Barrack Obama, in his remarks on February 1, 2011 to the Washington Press Pool regarding the crisis situation in Egypt, proclaimed that "…an orderly transition must be meaningful, it must be peaceful, and it must begin now."[23] The news media spotlighted the word "now" and prodded the President to clarify exactly what he intended by its use. Again another example of practicing "me" centered communication versus "we" focused communication. The President's use of the word "now" was ambiguous. What did he mean by "now?" His speech generated a barrage of questions, not only from the news

media, but from the global audience. The President, as was the case with Congressman Cohen, incorrectly assumed that "communication is the transfer of meanings from person to person."[24] President Obama and Congressman Cohen, like many leaders and communicators, assumed that the American, Egyptian and global audiences are passive in their listening. They failed to realize that communication centers on people, and that the meaning is in the receiver, not the messenger. These two examples of diplomacy and SC support Joseph Nye's view that "great powers try to use culture and narrative to create soft power that promotes their advantage, but they don't always understand how to do it."[25]

In his essay, "Strategic Communication: Getting Back to Basics," Admiral Mullen advocates that actions speak louder than words and that actions must always match one's words and vise a versa. Leaders must take the time and effort to build trust and relationships with those people and groups with whom they communicate. He stresses that good communication is reliant on "having the right intent up front and letting our actions speak for themselves."[26] He is accurate on all points. However, he fails to stress that leaders must understand that the interpretation of those actions, or words rest, not with the sender, but with the receiver. People and groups are fragmented, geographically and socially and connecting with them through either words or actions is not as easy as it sounds.[27] From his article, it can be inferred that leaders understand the purpose of communication. Admiral Mullen contends that the reason why leaders struggle with SC has less to do with understating how to communicate and more to do with understanding policy. He asserts that leaders should focus more on what their actions communicate, and less about how to communicate.[28] Actions along with credibility are undeniably important, but to separate it from the communication process is to err. Communication scholars would argue "audiences determine meaning by interpretation of our communication with them; thus what we say, do or show may not be what they hear or see."[29]

If leaders understand the communication process, the act of ensuring one's actions compliment their words will not be a challenge. Berlo posits that 1) people can have similar meanings only if they have

shared similar experiences; 2) meanings are not static, they change with experience; and 3) no two people can have exactly the same meaning for anything.[30] His final point resonates with the Bush Administration's communication strategy immediately following 9/11.

President George W. Bush and Secretary of State Condoleezza Rice used terms like democracy and freedom as part of their SC strategy, ignoring how these two words had different meanings not only with the American people, but those around the globe.[31] According to communication experts Aaron Hess and Z.S. Justus, choosing the correct word or words is critical when communicating, and using the wrong words can lead to a misunderstanding of those receiving the message. Hess and Justus assert that, "…war metaphors and language, such as victory, enemies, and allies occlude the reality of counterterrorism efforts."[32] Using the Bush Administration's narrative to describe the Global War on Terrorism as an example, it communicates a set of preconceived conditions that are associated with war in the cognitive framework of the majority of Americans and ignores those living in the Middle East.

Communication scholars Corman, Trethewey, and Goodall assert that describing the war on terrorism using language associated with past wars, i.e., World War II, leads people to expect the same result.[33] Leaders must understand that receivers of information are not processors or dictionaries. People and/or groups are not passive in the communication process, but are active interpreters of culture, behavior, and external sensors all of which contribute to their understanding. In order to understand communication, leaders must break away from the simplistic view of communication and "move toward a more complex appreciation and understanding of the communication process, as one that is always audience based, culturally dependent and meaning-centered."[34]

One technique leaders can use to assist them in improving their understanding of the complexities of the communication process, and their environment is called sensemaking. Just as the concept of design is used by leaders to develop a holistic view of the operational environment, sensemaking is a collaborative process of creating shared awareness and understanding from different individuals or groups'

perspectives and interests in that environment. It consists of the following seven properties:

- People rely on their environment to build their narrative.
- Retrospection is critical; it affects how people or groups view actions or events.
- Sensemaking is a social activity where people and groups share ideas and narratives. The conversations are never static; they are always changing.
- It is continuous. It causes people and groups to shape and frame their narratives in concert with their surroundings. As people or groups become exposed to their environment or surroundings, they build context that helps influence their understanding.
- Context provides reference for connecting ideas to meanings; it assists people and groups in decoding, deciding and acting on communication.
- Identification is central to sensemaking. When people or groups know how they fit in, it helps shape how they interpret events.
- People and groups favor plausibility over the accuracy in their understanding of actions, events and contexts.[35]

Each of these seven elements overlaps with each other as people or groups engage in dialogue. It is important to note that, through individual interpretations of the communication narrative, the result is the continuous sensemaking of the actions, images and words.[36] Sensemaking provides leaders with a "lens" to see and understand the complexities of the communication process; it is a "way" to view communication from a "we" mindset vice a "me" approach. The human communication process and landscape are littered with ambiguity, cultural and political interpretations and perspectives. In order to develop and execute an effective SC plan and strategy, leaders must change their mindset of how they view and understand the communication process. They must approach communication with a holistic view, and apply those critical, creative and systems "ways" of strategic thinking throughout the process. It is time to throw-out the old and out-dated paradigms of the communication process and begin to accept the idea that words do not have meaning, people do.

Transform how Leaders Communicate.

If changing the mindset of how leaders view and understand the communication process is the first step, the next critical area is changing how leaders communicate. For decades, the dominate communication practice used by leaders has been the one-way influence model and today, this 20th century model continues to dominate U.S. strategic communication efforts with minimal effect. The model is based on the advertising approach of selling a product, except in this case it is a message. The model treats receivers of information as passive in their interpretation and fails to consider the many influencers, i.e., language, culture, and politics, which affect the environment. This communication model or practice was used by the Bush Administration after 9/11. The result was many of the words and messages used to unify support were interpreted in different ways among the global audience. The effect was that the messengers were seen as not credible, and their messages were discounted, changed and/or used against the U.S. These words and others coupled with the reliance on the one-way influence model contributed to the United States' ineffective SC efforts.[37]

The traditional one-way influence model continues to be the dominant approach to communicating in some U.S. senior military commands. At the United States European Command (USEUCOM) in Stuttgart Germany, the one-way influence model is the dominate method to communicate to various audiences.[38] Messages are developed and transmitted through a specific channel or medium. The meanings reside in the minds of the EUCOM leadership and interpretation is left to chance. The message is transmitted repeatedly using the same channel to the same audience over time. The assumption is that if the message is sent enough times to the selected audience, over time the message will achieve the desired result or effect. The fallacy with this process is that it assumes that the selected audience is passive in their interpretation and understanding of the action, message or image.[39]

The one-way influence model suggests that sending a message is the same as communicating a message; it confuses dissemination with communication.[40] Communication Theorist Wilbur Schramm referred to this as the "Bullet Theory of communication."[41] Communication is treated as a bullet, per se, and when it comes in contact with the

intended receiver it automatically transfers beliefs, feelings, knowledge and understanding.[42] The reality is that there is no one sacred message expertly crafted or articulated that can change how people or groups think and act. People and groups actively engage and evaluate both mentally and physically the words, actions, and images they encounter. They file them in a particular context based on their culture, experience, history and political understanding.[43]

USEUCOM is not alone in its use of the traditional one-way influence model. Leaders, both in the military and government, fell victim to the practice of how to create the perfect persuasive message, instead of concentrating on understanding the reality of the people, group or audience they are trying to influence.[44] People and audiences cannot be labeled as passive in their interpretation of the message. The understanding that "the enemy has a vote" has to be applied to the communication process in the same way planners apply it in the operational planning process. The intended person or groups receiving the information have a vote, and they bring with them their own context comprised of their own experiences, and cultural and religious identities.

Nowhere was the one-way influence model evident than when Karen Hughes, Under Secretary of State for Public Diplomacy and Public Affairs, embarked on a tour of the Middle East in 2005 to improve the image of the U.S. and to learn more about the culture and customs. Her intent was to spotlight the freedoms women in the U.S. possess and enjoy. Though the tour was also a vehicle to promulgate President George W. Bush's SC message, the result was disastrous because Hughes and others involved did not understand the communication process. She failed because of her reliance on the one-way influence model of communication and the Bullet Theory of communication. Hughes did not consider the cultural and social context of the Saudi women she engaged. She assumed that her message of freedom, democracy and equality would be interpreted in the same way it is by women in the U.S. What occurred was the opposite.[45] Hughes and her approach are not alone. Leaders borrow methods from advertising and public relations practices, treating people and groups as if they are synonymous to business markets. As previously highlighted, words like freedom

and democracy are ideas and cannot be packaged and marketed to vast audiences in the same way McDonalds or Pepsi advertises their products. People and groups "interpret messages in ways that fit the existing scheme, rather than ways that senders may intend."[46]

A critical initial step in the communication process and subsequently SC is "understanding the pictures in the heads"[47] of the people. The one-way influence model "fails because it does not recognize communication as a meaning-making process."[48] In order for leaders to succeed with their SC efforts, they should deemphasize controlling the message and replace repetition of actions and messages with variation, utilizing different channels or mediums to communicate.[49] Leaders are expected to communicate and engage. The outdated one-way influence model is a paradigm of the past, and leaders must embrace this change if they are to see their SC efforts succeed.

Standardize it in the PME Framework.

"Challenge disinformation." "Engage the population." "Consult and build relationships."[50] These are just a few of the 24 points from General David H. Petraeus, Commander, International Security Assistance Force/United States Forces-Afghanistan, memorandum titled – "Counterinsurgency Guidance." Besides being a tool or channel to communicate directly to the troops in his command, one can also deduce from the document his thoughts on communication. The document lays a contextual foundation for interacting and engaging with the people of Afghanistan, undoubtedly his number one audience. Throughout the document, the themes of partnership and relationship resonate, and it can be inferred that one of the cornerstones for successful execution of Counterinsurgency (COIN) is communication. "Earn the people's trust, talk to them, ask them questions, and learn about their lives…Spend time, listen, consult and drink lots of tea."[51]

General Petraeus advocates building relationships with the Afghans, but for leaders on the ground what does that entail? How does one effectively communicate and subsequently build relationships? Experts and theorists agree that communication is paramount, if not a vital component of the COIN's success or failure.[52] The field manual on COIN, FM 3-24 *Counterinsurgency*, highlights the importance

of communication with emphasis on actions, dialogue, two-way communication, engagement and relationships, but where the manual and General Petraeus fall short is an explanation of the "ways" (how to) to communicate. It is easy to tell leaders that communication is critical. The difficult part is putting it into action effectively. What does a leader or diplomat need to know before he sits down with a leader of a tribe, a governor or minister of defense? Without a mechanism or "way" to educate and demonstrate to leaders the viability of General Petraeus' points, it becomes just another brilliant idea.

> *American officers train for years on infantry tactics, how to maneuver on an enemy and lead soldiers into battle. But some of the most crucial challenges for American soldiers today may be the human interactions for which they are often less prepared.*[53]

The above quote resonates when it comes to the communication process. After nearly 10 years of war, military and civilian leaders have embraced the importance of culture awareness education and language training. If communication is woven throughout all facets of society and culture, why not standardize it throughout a leader's professional education and development? An institution, such as the Army, which prides itself on being people oriented, could enhance its leaders by teaching them about the purpose of communication and how to communicate effectively; how sensemaking works; the importance of perception; why relationships matter and how culture affects the communication process. The Army should incorporate the study of communication at the entry levels of professional military education and continue at the military's premier higher-learning institutions, such as the U.S. Army War College. War is complex for many reasons, but fundamentally it is complex because it involves people. To study communication is to study people. It is time the Army embraces the scholarship of communication with earnest and vigor.

Incorporate into Shaping Efforts.

The term "shaping" is not new; it has been a part of the U.S. military and government's lexicon for decades. It refers to those activities designed to limit an adversary's options or increase friendly force's options.[54] If culture, education, religion, and politics are critical to

both shaping and the communication process, why isn't the later identified as a key component of shaping operations? Helmus, Paul, and Glen deduce that the military faces four broad challenges with shaping operations: "anti-American sentiment; adversaries' shaping efforts; news and news media; context, including global media [and] local information; environment, culture and technology."[55] The purpose of communication is to influence. Nearly every action, image or message, can shape the opinions of a selected group or audience. If certain actions, words, or images do not translate well with the selected audience, communication could breakdown and shaping efforts fail.

As previously highlighted, the meaning of the message is in the people and not in the message. This is not only fundamental to the communication process, but shaping efforts as well. Shaping efforts, especially as they concern message development and acceptance, share the same elements of the communication process, i.e., culture, language, and environment. Helmus, Paul, and Glen contend that leaders cannot treat communication as a one size fits all concept. If this occurs, it could prove detrimental to shaping operations.[56] Leaders should integrate the communication process into their shaping operations starting with the cognitive application of design and continuing through the formal planning process, such as the military decision making process. This integration would allow leaders to understand the complexity of the communication process from interpreting an adversary's actions to making attributions about beliefs, motivations and intentions.[57]

Define the Communication Objectives.

A well developed SC plan and strategy will include communication objectives. These objectives will be linked to the overall desired cognitive effect on a selected audience. But when analyzing an audience or segmenting a particular group into like-minded or behaving groups, how can leaders go about developing their communication objectives to support their SC plan and strategy? The Behavior, Relationship, Information, and Motivation method (BRIM) is a "way" or tool to assist leaders.

The *behavior* objective is focused on changing the way people act or in some cases not act. The behavior objective is difficult because it

represents a lifetime of experiences, and normally requires time and effort to change or modify behaviors.[58] The key with behavior change is that the people or groups must first be informed and persuaded before any behavioral change can take place.[59] Persuasive communication requires some yielding on the part of the receiver and the dynamics by which the receiver may allow himself to be persuaded.[60] It is important to note that persuasion involves more than just developing a new and improved persuasive message; it requires an analysis of the person or group's system.[61] The following persuasive communication recommendations are offered by Scott M. Cutlip, Allen H. Center, and Glen M. Broom:

- If the receiver of the message is opposed to your position, frame the issue by providing both sides of the argument.
- If the person or group agrees with your position, ensure your arguments reinforce this acceptance.
- If the person or group is educated, include both sides of the argument, but avoid omitting any relevant information because this could be perceived as suspicious.
- If the person or group is likely to be exposed to messaging that counters your position, ensure countering with messages that build support and resistance to any type of counter messaging.[62]

The *relationship* objective focuses on the level and degree of the relationship that is desired with the person or group. These desired relationships could range from adversarial, noncommittal to a trusted partner. When all other shaping efforts have failed, and credibility is damaged from adverse actions or events, the established relationship objective is probably the most powerful and rewarding.[63] Communication in terms of relationships reflects four basic dimensions: emotional, intimacy, liking and submission. Communication in relationships not only reduces uncertainty, but it provides a fundamental ingredient for continuing the relationship. As previously noted, communication involves people and one cannot attempt to understand the communication process alone; it requires not only the relationship between the communicators, but how the communication occurs in the comprehensive social environment.[64]

The *information* objective centers on the knowledge people or groups have garnered as a result of communication. The process of informing people is not as easy as it implies because it involves the interpretation of one another's actions and creates perceptions about thoughts, motivations, and intentions.[65] The objective is to increase the audience's knowledge, awareness and understanding. The process of informing involves four steps:

1. To attract attention to the communicator;
2. To have it accepted;
3. To have it interpreted as intended by the communicator;
4. To have it stored away by the receiver for later use.[66]

The desired effect is the audience takes action (if this is the objective) because opinions and behaviors have been influenced as a result of this knowledge, awareness and understanding.[67]

The last communication objective is *motivation*, and quite possibly the hardest to achieve. There are many factors that are uncontrollable, such as what motivations in terms of attitudes, beliefs, opinions and actions are desired. For example, an SC strategy may seek to have a foreign minister of defense publicly acknowledge to the news media the benefits of a joint military training venture between his country and the U.S. This leader's motivation to act is the result of increasing the foreign minister of defense's knowledge or changing his behavior. The BRIM method is a tool that can assist leaders during the application of design as well as throughout the military decision making process. It is a "way" to assist leaders in articulating the desired cognitive effect of an audience and achieve the SC goal.

Conclusion

Leaders, military or civilian, are expected to succeed in volatile, uncertain, complex and ambiguous environments wrought with friction and tension. Human variables, interactions, and relationships will always dominate the landscape as they have for centuries. It is because of these human variables that effective SC is essential in order to support national and military strategic objectives. In his speech at

the Association of the United States Army Conference in October 2007, Secretary of Defense Robert Gates stated that success as a nation and military will be determined not on the use of military force or power, but more of shaping the behavior of our adversaries, allies and all those citizens caught in the middle.[68] Strategic communication will require a substantial investment, by leaders, in the communication process. The war of ideas, battle of the narratives, or the winning of hearts and minds has many things in common, but the one thing that links them is communication. Communication and action are not the ends, but only the means to achieve the desired ends.[69] If these desired ends entail changing behaviors, beliefs or perceptions, understanding the human communication process must be at the forefront of SC. In this global information age, more than ever, leaders must understand that relationships matter, the communication narrative is not one size fits all, that controlling the message in a country we do not understand and a language we do not speak is futile, and focusing on cooperation and listening vice power and dominance is the best alternative.

Section Three

Information Sharing


U.S. ARMY WAR COLLEGE
Prudens
Futuri
Carlisle Barracks, PA

Introduction

Information sharing is critical to success in today's joint, interagency, intergovernmental, and multinational environment. As senior leaders face this complex environment they must weigh the benefits of information sharing along with the risks. Providing intelligence information to our partners, both at home and abroad, requires not only a change in policies and processes but also a change in culture. The *Intelligence Community Information Sharing Strategy* reminds us that, "the risks associated with not sharing can lead to missing clues of an attack, cost lives, and endanger our Nation's security." The strategy calls for a shift from the Cold War 'need to know' mindset "to a 'responsibility to provide' culture…predicated on managing risks associated with mission effectiveness and unauthorized disclosure of sensitive information."[1] This section includes student essays that highlight shortfalls and recommend improvements to information sharing in the domestic and multinational environment.

In his award winning essay, "DOD Information Sharing with Domestic Emergency Partners for Defense Support of Civil Authorities Missions," Colonel Robert Hedgepeth identifies the need for improved information sharing with federal, state, and local government agencies as well as non-government and private volunteer organizations and corporations. He states that U.S. military organizations providing support must proactively identify and implement ways to collaborate and share information with other domestic emergency response partners, including the public, while protecting and defending military networks. At the same time, these non-military partners should coordinate with the Department of Defense to establish terms and conditions for data sharing relationships prior to an incident. Colonel Hedgepeth recommends policies for forming ad-hoc relationships and emphasizes the importance of strengthening relationships to ensure an informed response at critical times when lives and property are at stake.

Colonel Jonas Vogelhut explores multinational information sharing issues in his essay, "Coalition Mission Command: Balancing Information Security and Sharing Requirements." He points out the

challenges government policymakers and military commanders face as they attempt to balance the need for information sharing with the imperative to protect operational security. He analyzes the Afghan Mission Network (AMN), to identify areas for improvement. He examines current policy and international agreements and recommends that U.S. senior leaders develop and implement policies, processes, and technologies to share sensitive mission information with coalition partners while protecting against unauthorized releases that jeopardize operational security.

These excellent papers provide a depth of research and thought concerning improvements in domestic and international information sharing. They lay the groundwork for the development of new and innovative ideas to enhance coordination and ultimately mission success in today's complex and challenging environment.

DOD Information Sharing with Domestic Emergency Partners for Defense Support of Civil Authorities Missions

Colonel Robert A. Hedgepeth
United States Army

Federal, state, and local government agencies as well as non-government and private volunteer organizations must establish relationships and mechanisms for information sharing prior to disasters. These organizations should periodically review and maintain information sharing initiatives for use during DOD homeland defense and disaster relief missions to assure a fully coordinated response in a timely manner with DOD partner organizations. At all levels, the DOD must proactively establish and maintain these relationships to enhance informed decision making and performance of domestic operations.

The Department of Defense (DOD) provides support to civilian authorities after natural disasters and when the security of the U.S. requires augmentation by the military forces to save life and limb and to protect critical infrastructure.[1] In all cases, and in accordance with the U.S. Constitution, the military assistance provided is in support of civil authorities.[2]

This support is provided to civil authorities in accordance with Homeland Security Presidential Directive 5[3] which establishes the Department of Homeland Security's (DHS) National Incident Management System (NIMS). NIMS is a key part of the National Response Framework and "[e]stablishes a systematic approach for managing incidents nationwide."[4] It is coordinated with the National Strategy for Homeland Security and Response Partner Guides. These guides define "key roles and actions for local, tribal,[5] State, federal, and private-sector response partners."[6]

DOD provides support in a scalable manner, although rules governing assistance requests vary from state to state. Small responses usually

involve requests elevated from county (or equivalent) emergency management coordinators to an agency representing the state's governor. The governor may then provide National Guard assistance to work alongside other agencies who are either responding at the direction of the governor or via separate mutual aid agreements.[7] The National Guard usually performs assistance in a State Active Duty status, funded directly by that state's government, or federally funded in Title 32 status.[8] If the President declares the incident a federal disaster, the federal government will reimburse at least a portion of state funds expended for this purpose.[9]

A typical National Guard response might include aviation, engineer, medical, communications, transportation, and logistics support as well as trained and disciplined manpower for security and presence patrols, along with headquarters elements to provide command and control of military assistance forces. These missions exemplify the concept of 'dual-use;' the application of the military's warfighting training and equipment for a military supported domestic response.[10]

States may execute an Emergency Management Assistance Compact (EMAC) to provide interstate mutual aid of civilian and military capabilities if the scope of the disaster surpasses a state's ability to respond. The agreements define the terms and conditions of support, liability, and fund reimbursement.[11]

An even larger disaster, one that exceeds the capacity of local and regional assets or requires special capabilities, may involve a federal response. This response is typically made under the provisions of the Stafford Act,[12] which allows the President to direct the use of DOD resources to perform emergency work "which is essential for the preservation of life and property."[13] At this point, United States Northern Command (NORTHCOM) will involve active duty and reserve forces in a Title 10 status, provided in a supporting role to civilian authorities as well.[14]

Examples of Defense Support of Civil Authorities (DSCA)[15] missions for relief following natural disasters range from requests for National Guard assistance at the local, county, tribal and state levels for tornados, winter storms, and floods to full scale, Title 10 and 32 responses for catastrophic events. Hurricane Katrina, which dramatically affected

the Gulf Coast in 2005, is an example of such a catastrophic event. The state and federal response to Katrina included approximately 72,000 military personnel,[16] and was the largest DSCA response in U.S. history.[17]

Responses requiring personnel and equipment in numbers comparable to the Katrina response could also be required in homeland defense situations. These incidents involve a manmade or natural threat or attack within the United States, such as those occurring in the aftermath of the September 11, 2001 terrorist attacks or a large, widespread Chemical, Biological, Radiological or Nuclear (CBRN) incident.[18] Together, homeland defense, natural disasters, and other "equivalent emergencies that endanger life and property or disrupt the usual process of government" are termed domestic emergencies.[19] In all cases, numerous government, charitable and private organizations conduct disaster relief at all levels.

> *Citizens are not well served if disaster response is not based on the joint, interagency, inter-governmental and multi-national (JIIM) partnership….It is wasteful and counterproductive not to engage early and regularly with civilian and military partners who, acting synchronously, provide valuable mutual assistance to one another.*[20]

Information Sharing

One large part of 'acting synchronously' during domestic emergencies is the exchange of electronic information between the many entities responding to the incident. Former Vice Chairman of the Joint Chiefs of Staff, General James Cartwright, in speaking of the military's capabilities to share information with partner agencies, reinforced the similarities between offensive operations in Afghanistan and Iraq and DSCA missions. In theater "…we fight interagency and coalition,"[21] he said, emphasizing the close relationships between U.S. military forces and other partners. Similar relationships hold true for DSCA missions.[22]

Flexible, open communication systems and widespread sharing of information is contrary to most actions required to ensure the integrity and security of information systems. DOD goes to great efforts to

protect and defend its networks and data from intrusion, attack and tampering. Policies exist to govern accessing, reception, sharing and transmitting files within and outside the DOD network domain. DOD elements must proactively engage with partner agencies to define the terms and conditions of information sharing. DOD and partner organizations must define standard operating procedures and technologies to avoid unnecessary planning in the midst of a domestic emergency.

Much of the criticism related to the federal response to Hurricane Katrina linked to "significant organization and coordination problems" and lapses in communications and situational awareness.[23] Failure to plan and conduct proper coordination for future incidents will continue to contribute to unacceptable delays and deny critical planning information from those charged with making decisions and saving lives.

This coordination may include guidelines for permissible file formats, hardware and software security settings, definitions of document designations, and instructions for handling and disclosing information to others. Some commonly encountered types of information requiring designations include: controlled unclassified information (CUI)[24] such as sensitive information,[25] operational and tactical information, Law Enforcement Sensitive (LES) information; personally identifiable information (PII); Protected Critical Infrastructure Information (PCII),[26] and information that may be subject to protection under the Health Insurance Portability and Accountability Act (HIPAA).[27] This coordination should also cover the designation and handling of information labeled 'For Official Use Only (FOUO)' under the requirements of the Freedom of Information Act (FOIA).[28]

Delineating exactly how these information exchanges take place during DSCA response situations demand a basic mission analysis: **who, what, why, when, where and how**, by domestic operations planners in conjunction with points of contact at partner agencies.[29] Once organizations resolve these questions for mission planners, then a framework for coordination can be established and executed to ensure timely and secure information flow with domestic emergency partners during DSCA missions.

- Who are likely partners that need or have relevant information?
- What types of critical information are expected to be shared with others?
- Why is the information necessary?
- When will the information be needed?
- Where will the information be needed?
- How will the information be coordinated, transmitted, received and used and how will the integrity of the information be maintained?

Who

Who are likely partners that need or have relevant information? Military forces may send and receive information to and from many different and varied entities outside the DOD network domain.[30] These entities may include other government organizations (OGO), foreign government or military organizations, non-governmental organizations (NGO), private volunteer organizations (PVO), corporate partners and the public.

Some of these potential partners may seem unlikely to traditional emergency response planners. One usually associates the U.S. military with helping other countries during natural disasters, not the reciprocal. In the aftermath of Hurricane Katrina the United States did receive assistance from the governments and militaries of Mexico[31] and Canada.[32] Canada assisted the United States before, and a Strategic Operations Information Sharing Plan of Action exists between the two nations.[33] This event set a precedent for Mexican assistance and reinforces the requirement for multi-national cooperation.

Another group of seemingly unlikely disaster relief partners include corporations. Walmart is the world's number one retailer, with over 2.1 million employees and to almost 9,900 stores.[34] According to Brian Koon, Director of Emergency Management for Walmart, the corporation set a new precedent for private sector emergency management in the aftermath of Hurricane Katrina. Katrina damaged over 120 Walmart stores, but they mobilized their corporate logistics system to set up temporary stores in parking lots of their damaged or

destroyed properties. Walmart sold or donated nearly 2,500 truckloads of merchandise for survival and recovery efforts.[35]

Walmart realized detailed coordination with other entities and officials would help to serve a larger population of the disaster population. An example of wasted resources cited by Koon relates a water distribution point set up by emergency management facilities in the same parking lot as a temporary store, which also had supplies of water. Meanwhile, other areas in the same county were more than ten miles away from any water distribution points. The point Koon makes is that Walmart and emergency management officials should share data about where they were distributing supplies to reduce duplication of effort to better accommodate other areas.[36]

Townsend and Moss, in their analysis of telecommunications in disasters, quote researchers of Japan's 1996 Kobe earthquake:

> *The basic lesson from Kobe is that the usual approach of disaster communications, traditionally based on military-style public safety agencies that are operating in a topdown manner and share information with "civilians" only on a "need-to-know" basis, should be replaced. Instead, we should set up an open-access emergency system - open to inputs from a wide variety of public and private participants and with open to access to that information.*[37]

While the Kobe article focuses specifically on voice telecommunications, Townsend and Moss' research also analyzed telecommunications systems and their uses during other significant incidents. They examined the 2004 Indian Ocean Tsunami, the September 11, 2001 terrorist attacks on the World Trade Center, and the 1999 NATO bombing of Belgrade.[38] During this time, the use of cellular telecommunications for voice and data services expanded greatly. They found that:

> *Three decades of social science research in disaster recovery has produced a compelling body of evidence on the important response role of private firms, NGOs, and social networks.*[39] *International aid agencies are increasingly orienting disaster preparedness and prevention strategies around these institutions.*[40] *Particularly in very large or prolonged disasters that exhaust official capabilities, NGOs and citizen volunteers are crucial.*[41]

The mention of social networks in this 2005 effort is very interesting. As technologies continue to develop, social networking is playing an even larger role in emergency management. Social networking and interested volunteer communities around the world played a very important role during the 2010 earthquake in Haiti and the 2011 earthquake in Christchurch, New Zealand.[42]

Many different entities have the capabilities and will to assist during domestic emergencies. It is difficult to anticipate which partners will respond to an emergency, regardless of the size of the event. As the next section shows, common points of coordination must be determined to make those initial meetings smoother.

What and Why

What types of critical information should organizations expect to share with others and why is the information necessary? Electronic information types likely to be shared during domestic response operations might typically include common word processing, spreadsheet, presentation files, graphics and geo-tagged[43] information used to create common operating pictures.

Accurate and verifiable data that supports responders, decision makers and planners will assist in delivering aid to those affected by catastrophe. This information may include orders, situation update reports, logistics requirements, pictures, videos, briefings and the status of personnel, equipment and supplies. Important information may be accessed though: email text and attached data files; files made available on web-based file sharing portals; partner incident management systems; partner mapping solutions and social media information from Facebook and Twitter.[44]

Basic email and email with file attachments are the simplest exchanges of information, but they are not without complications. Organizations need to address standard operating procedures regarding email use prior to a domestic emergency. Some federal, state and local government agencies as well as non-government and private volunteer organizations require encrypted messages and attachments originating from their networks. This may render the messages unusable by recipients off

the domain. Other networks, including the military, block certain types of attachments, such as compressed files commonly known as zip files. Files of this type have the potential to mask viruses which would otherwise escape detection until set forth to damage network or corrupt data. Simply knowing that a system will not accept these types of files is valuable; helping other users understand alternate methods of transmission are required.

RECOMMENDATION: Coordination between agencies should include an understanding of the basic capabilities these partners will employ to ensure compatibility for viewing and editing, knowledge of bandwidth limitations, limitations on file sizes of user mailboxes to send or receive, and directories of user names, positions or responsibilities, email addresses and telephone numbers for use during the emergency.

Maintaining email and telephone directories with frequent updates is also important; especially as personnel change duties. Organizations may have to shift responsibilities based on who is actually available to participate in a disaster response. This is especially true for responders located close to the event, as some people may be personally affected by the disaster and unavailable to perform their normal response duties.

Web-based file sharing portals, such as Microsoft SharePoint,[45] allow users to seek out information posted in a pre-arranged location, instead of relying on the originator to send out the information attached to an email. SharePoint allows tiered access ranging from unrestricted public access, to password protected internet users, to restrictions allowing only intranet or domain user access. Access to SharePoint websites requires prior coordination to ensure security protocols and web browser settings are compatible. Institutions must provide more training for SharePoint users to understand where and how to store information, and what privileges they have on the site related to reading, modifying, posting and sharing documents. Users may also receive email notifications when others post new or updated documents.

Incident management systems typically include web-based tools to: log incident information, track requests for materials, assistance and information and provide electronic chat services and chat logs for

incident managers. The systems may include useful information such as mission tracking numbers, locations, point of contact information and specific mission requirements and approvals. Access to this data is vital for military agencies partnering with emergency managers to achieve situational awareness and common incident understanding.

ESI's WebEOC[46] and E Team's NC4[47] are examples of commercially available incident management systems in use by many federal, state and local agencies as well as private corporations. Access to incident management systems is typically password protected and may require training on specific features or agency standard operating procedures. Some of the information contained in these incident management systems can be displayed graphically, or exported to other mapping systems to allow users to ascertain the status of information linked to particular locations.

The National Guard Bureau uses the Joint Information Exchange Environment (JIEE) to maintain situational awareness for tracking alerts, missions and assets around the country although not intended for use during incident management. JIEE facilitates requests for information and assistance among state National Guards and National Guard Bureau and provides visibility of these activities to NORTHCOM, DHS and FEMA.[48]

Partners can share geospatial information related to an incident or the area around an incident site to build a Common Operating Picture. It is not 'common' in the sense that each user sees the same picture. It is common in that each user determines the most important information to meet their needs, based on manipulation of layers containing identical data. Organizations have the ability to hide information so as not to obscure or clutter their map. The Federal Emergency Management Agency's (FEMA) National Emergency Communications Plan (NECP) defines Common Operating Picture (COP) as:

> *offer[ing] a standard overview of an incident, thereby providing incident information that enables [all involved] to make effective, consistent, and timely decisions. Compiling data from multiple sources and disseminating the collaborative information COP ensures that all responding entities have the same understanding*

> *and awareness of incident status and information when conducting operations.*[49]

One can find Common Operating Pictures on today's digitized battlefield with military systems such as Blue Force Tracker, Maneuver Control System, and Movement Tracking System. These systems depict locations of units, equipment and supplies on maps or satellite overlays. The concept of COP is also gaining popularity in emergency management. COP displays information graphically, and into layers by subject. Just as layers of acetate and symbols can be placed over conventional paper maps to display items of interest, electronic mapping layers can be turned on or off to show different information over background maps or imagery.

The COP information and the resulting layers are managed with mapping software such as ESRI's ArcGIS,[50] favored by GIS professionals, and Google Earth,[51] which is readily available and free. WebEOC and JIEE both offer the option to represent information contained in their incident management systems geospatially. Users can import and export information points or layers in standard file formats common to GIS mapping systems.[52] Points of coordination related to these data exchanges include formats, methods and locations where layer files will be exchanged, and intervals that data will be updated to ensure that the latency, or delay from real time is known to all parties.

The development and use of Common Operating Pictures took on an entirely new dimension during Haiti's earthquake in January 2010. This devastating 7.0 magnitude quake killed more than 230,000 people.[53] Nelson and Sigal wrote:

> *The relief efforts became a living laboratory for new applications such as SMS (short message service) texting, interactive on-line maps, and radio-cell phone hybrids. These tools were applied to urgent tasks such as guiding search-and-rescue teams, locating missing persons, and delivering food and water to the populations that needed them the most.*[54]

Shortly after the disaster, the Haitian cellular telephone network began to come back on line to include basic text messaging (Short Message Service or SMS). Humanitarian organizations worked to institute an

SMS short code[55] that enabled cell phone users to communicate with aid workers. "Reports about trapped persons, medical emergencies and specific needs such as food, water and shelter were received and geo-tagged on maps updated in real time by an international group of volunteers."[56] Within days, "thousands of messages were coming through the system."[57]

Creole speakers from around the world volunteered to translate the text messages and provide them back to rescue workers. Another group of volunteers at Tufts University in Boston began using the crisis mapping program Ushahidi,[58] originally developed to map political violence in Kenya, to publish locations where people were trapped and to depict where aid was available. A third volunteer group from the Georgia Institute of Technology converted Ushahidi data to KML for use with Google Earth. The smaller file formats allowed responders with bandwidth restrictions, in this case the U.S. Marines, to receive and use the data.[59]

The Ushahidi platform was used for similar purposes after a 6.3 magnitude earthquake struck Christchurch, New Zealand in February 2011. It allowed users to track the availability of medical and humanitarian aid, government notices, building inspections, and utility restoration efforts in different areas of the city.[60]

The Ushahidi maps for Haiti and Christchurch also included information gathered from the social media sites Facebook and Twitter.[61] On-line volunteers around the world turned social media reports into posts located on the Ushahidi map. Responding organizations used a process to filter information, eliminate duplicate items and verify facts to lend validity to the information.[62]

Civil and military responders recognize social media as a source of intelligence. FEMA Administrator Craig Fugate, in an address to a Senate sub-committee, said,

> *…individuals, families and communities are our nation's 'first' first responders. The sooner we are able to ascertain the on-the-ground reality of a situation, the better we will be able to coordinate our response effort in support of our citizens and first responders. Through the use of social media, we can disseminate important*

> *information to individuals and communities, while also receiving essential real-time updates from those with first-hand awareness.*[63]

Twitter is especially valuable as it allows a user to search for and follow incident information. While any single user's eyewitness account of an incident or event may not be credible, the technique of "crowdsourcing"[64] allows analysis of multiple reports of the same occurrence, increasing the credibility of the information.

The United States Southern Command (SOUTHCOM) uses social media to "provide greater situational awareness to facili[ta]te faster responses."[65] Employing a Twitter search dashboard called TweetGrid,[66] their Operations Center learned of the Haiti earthquake while the ground was still shaking, well before news organizations. Similarly, FEMA made use of Twitter after the East Coast earthquake in August 2011 to determine the extent of tremors when cell phone networks were unavailable.[67]

Social media also can allow emergency managers and their public information officers easy avenues to communicate pertinent information to the public without having to wait for the traditional print or broadcast media news cycle. Immediately after the Christchurch earthquake responders used Twitter to direct people to areas of shelter, fresh water and clothing distribution points and to relay information about the restoration of utilities. This technique of information dissemination was used after the May 2011 tornado in Joplin, Missouri.[68]

The task of caring for victims can become easier by canvassing partner agencies and the public to determine the most appropriate and necessary information, and by quickly making that information available to the people affected by the disaster. NIMS calls for the establishment of a Joint Information Center (JIC) and for public information to "be coordinated and integrated across jurisdictions and across jurisdictions, agencies, and organizations; among Federal, State, tribal, and local governments; and with NGOs and the private sector."[69] In many cases, the public affairs capabilities the military brings to a disaster will greatly assist the JIC mission.

Disaster response information can take many forms. Although programs and platforms will continue to change, and innovations will continue to advance, planners must remain flexible in their approaches and keep in mind that coordination is key to their ability to partner with other agencies.[70]

When and Where

When and where will the information be needed? Most information exchanges occur via the Internet; beginning in some cases even before a domestic emergency event occurs.

RECOMMENDATION: Regular and routine access to systems and password protected accounts must be maintained as part of steady state operations to ensure availability whenever required.

Access to information related to emergencies may be required from the highest levels of government to responders on-site and to the public. Many important decisions related to resourcing and supplying disaster areas are made in operations centers that located a great distance from the incident site or affected area. Decision makers at a distance are relying on information gained from those present at the incident site as a basis for their judgments.

It is important to make available the most credible, clear, concise and correct information to partners so they may maintain situational awareness and make timely, quality decisions. It is also important that easily attainable, appropriate information be available to the pre-staged or on-site response partners who may face challenges due to disaster related service interruptions, overloads in internet and cellular phone services, or have equipment with limited connectivity.

Although the use of cellular services ultimately proved resilient in Haiti, the earthquake destroyed many cell towers when the buildings that supported the towers collapsed. In other cases, tremors shook the system components out of alignment and required attention from technicians before they could be put back into operation.[71] Because of the limited availability of the system, and the lower quality of service requirements for data as compared to voice traffic, the SMS text

messaging employed was very successful for communications in the affected area.[72]

Data takes on many different forms for many different users, but it is undisputed that appropriate data reach the response partners. It also holds true that timely data is required throughout the entire cycle of an incident.

How

How will the information be coordinated, transmitted, received and used, and how will the integrity and security of the information be maintained?

RECOMMENDATION: The military and other agencies likely to respond to disasters must build relationships at all levels to ensure they are ready to work together.

At the federal level, the 2010 Quadrennial Defense Review calls for the improvements in DSCA support and states, "the Department of Defense will closely cooperate with other U.S. departments and agencies to better protect and advance America's interests."[73] To this end, DOD and DHS are in the process of implementing a Strategic Operations Information Sharing Plan,[74] and the Secretary of Defense has convened a Defense Science Board Task Force on Achieving Interoperability in a Net-Centric Environment. Their product dives deeply into technical issues focused mainly on DOD interoperability, but also considered DHS interoperability during domestic emergency response.[75] This level of interagency cooperation calls for formal agreements, governance, testing and accreditation. Organizations must also consider smaller scale information sharing relationships.

It is essential that state, tribal, and local[76] level entities strengthen their abilities to work together, and with private and public entities at their levels. The National Fire Protection Association (NFPA), an internationally recognized code making body recognized as an authority for reduction of the burden of fire and other hazards, created Code 1600, the *Standard on Disaster/Emergency Management and Business Continuity Programs*. It advocates coordination and advisory committees

as well as training and exercises to prepare for the implementation of disaster plans.[77] Similarly, recommendations resulting from the 2010 Haiti earthquake include "engag[ing] in preparation and simulation exercises…for future emergency responses…to identify models for how formal institutions and self-organized efforts on the ground interact during humanitarian response."[78]

One important aspect associated with information sharing for the myriad of disaster response partners is establishing mechanisms to trust other users to ensure information integrity. In this context, a trusted entity is one that provides some assurance that the sender or receiver of information is actually who they claim to be, based on their user name or account name. Untrusted entities may not necessarily be who they claim to be when there is no mechanism for verification.

DOD user trust is based on a non-repudiation mechanism provided by a unique and private key held by each user's common access card and a personal identification number. This assures senders and receivers of email messages actually came from a named user's account. Other users with government or corporate domains may have assurances built into their processes that make it likely that a user is actually who they claim to be. Public email services such as G-mail or Hotmail,[79] offer no such means to validate user names.

It is possible to maintain information flow to and from untrusted users, but trusted users may benefit from access to additional information, such as CUI or otherwise sensitive information that is restricted to others. Guidance for information classifications, handling and access should be another point of coordination among partners.

During their response to the Haiti earthquake, SOUTHCOM established a Community of Interest (COI) on the All Partners Access Network (APAN). APAN is a file sharing portal created to provide "effective information exchange and collaboration between [DOD] and any external country, organization, agency or individual that does not have ready access to traditional DOD systems and networks."[80] Another such endeavor by the DOD's Joint Knowledge Online (JKO), is HARMONIEWeb. It provides an environment to "forge trusted working relationships between government and non-government

organizations in a trusted environment.…while keeping out those whose interests are not so noble."[81] Both sites employ techniques to validate users or domains to limit the access of untrusted entities.

DHS has established similar capabilities in the Homeland Security Information Network (HSIN). It "is a national secure and trusted web-based portal for information sharing and collaboration between federal, state, local, tribal, territorial, private sector, and international partners engaged in the homeland security mission."[82]

Each site offers a slightly different collection of tools for communicating and sharing information related to disaster management. Some individual states have also undertaken efforts to provide information sharing platforms for partner agencies.[83]

RECOMMENDATION: Arrangements to credential the most likely partners or domains should be included in early coordination efforts.

Other coordination points for local and regional partners include email communications and file sharing portal access, regular directory maintenance, understandings of file types and sizes to be exchanged, and estimations of bandwidth capacities that users expect to have available. They may also include password protected access to Incident Management Systems, and guidelines for monitoring or using the information contained on those systems.

RECOMMENDATION: These points should be written into EMAC agreements or memorandums of understanding between partner agencies.

Similar points also accompany layer sharing for common operating pictures. DOD's APAN, the National Guard's Geospatial Information Center (GIC),[84] and a DHS product called Virtual USA[85] provide common interface points for such layer exchange. Other, similar endeavors include NORTHCOM's Situational Awareness Geospatial Enterprise (SAGE),[86] DHS's Integrated Common Analytical Viewer (iCAV), and DHS Earth, providing access to many critical infrastructure and homeland security related data layers.[87]

Responders close to disaster areas may count on cell phone networks as their primary mode of voice and data communications. Even though networks make efforts to harden their systems and provide redundancy, network availability may not be a realistic expectation immediately after the disaster. In some cases, cellular companies may bring in portable cellular assets to supplement or replace damaged parts of their system,[88] leaving those voice and data services degraded in the hours immediately after the incident. Coordination with these service providers may aid in infrastructure restoration that is critical to responders.

Responding agencies and their counterparts should understand how communications degradation may affect them in the first hours after a disaster. Coordination with other partners to share satellite access may be very valuable. Because of the possibility of limited availability of cell networks, SMS text messaging in lieu of voice operations also proves viable. SMS facilitates automatic resending data if the first transmission is unsuccessful. Cellular systems also have the capability, if configured appropriately, to accommodate bulk message broadcasts in a manner that minimizes the effect to the cellular network.[89] Knowing which agencies and numbers are equipped to receive SMS text messages is certainly a valuable planning point as well.

Incorporating social media before disaster strikes involves establishing accounts and gaining and maintaining a following of partner agencies and users by establishing a presence on the services and providing useful information on a regular basis. This could include reposting useful information from partner agencies social media sites and inviting local news media to follow and repost pertinent information.[90] During a disaster, early monitoring of social media messages and establishment of simple keywords (called hashtags[91]) is vital to gain new followers and increase the span of coverage. Twitter offers a feature for users to monitor trends in hashtags to maintain awareness of popular topics.

Trusted user status is very difficult on social media such as Twitter. The site has had a process in place to verify or trust users claiming to be celebrities. It may be possible, in the future, for public officials and disaster response agencies to petition for similar status. In the meantime, Twitter recommends users link to a Twitter identity from an official website.[92]

Putting trust in individual social media users is even more difficult for emergency managers and partner agencies, and manually evaluating this data can be time consuming. The creators of Ushahidi have developed a free, open-source product called Swiftriver to sort and filter data and impart a degree of trust and verification into crowdsource data. It was "born out of the need to understand and act upon a wave of massive amounts of crisis data that tends to overwhelm in the first 24 hours of a disaster."[93] "The software…is based on the idea that by comparing messages and information from a variety of sources about an incident, the system can build an understanding of which are credible and which are not."[94]

RECOMMENDATION: Organizations should explore the tools described above before disaster strikes to build operator proficiencies. The operational tempo after an incident is sometimes too high to allow for the associated learning curve.

Conclusion

Early establishment of partner relationships and periodic contact to maintain coordination is vital to successful working relationships and information sharing mechanisms. Domestic operations partners, including military elements, must be cognizant of the fact that it is impossible to imagine every partner agency to be involved before the disaster strikes. Planning and training on new partner coordination may make these actions easier after the disaster.

The need for information sharing among domestic operations partners is apparent, and the requirements seem to be growing almost as fast as solutions are developed or adapted. It is essential for planners to focus on interoperability and flexibility, steering away from proprietary systems and other limiting factors that may preclude adaption as technology changes. This will better facilitate interoperability with other response partners.

Certainly, organizations must develop pre-established relationships and mechanisms for information sharing prior to disasters to save valuable time in the crucial hours immediately after disaster strikes. DOD must proactively engage their most likely response partners

to build relationships and begin coordination efforts. Federal, state, and local government agencies as well as non-government and private volunteer organizations should periodically revisit relationships and standard operating procedures to ensure that the homeland defense and disaster relief responders are prepared and equipped to aid in a fully coordinated response by exchanging appropriate information in a timely manner with DOD partner organizations.


U.S. ARMY WAR COLLEGE
Prudens
Futuri
Carlisle Barracks, PA

Coalition Mission Command: Balancing Information Security and Sharing Requirements

Colonel Jonas Vogelhut
United States Army

The 2010 U.S. National Security Strategy states that "the foundation of United States, regional, and global security will remain America's relations with our allies, and our commitment to their security is unshakable."[1] The 2008 *National Defense Strategy* reinforces this imperative by stating victory against violent extremist groups and other threats require the United States to "apply all elements of national power in partnership with old allies and new partners"[2] and that "the long war is ultimately not winnable without them."[3]

As future military operations expand participation in coalitions rather than single-nation efforts, policymakers and commanders will continue to face the challenge of choosing when and how much information to share to be effective. Idealistically, sharing all information with coalition partners would enhance overall situational awareness and improve decision making by creating a common operational picture. However disclosure of too much information (e.g., friendly force locations) may also threaten operations, leaving coalition forces vulnerable to attack and weakening mission effectiveness.

Historically, coalitions primarily shared information through active delivery of information. Liaison officers stationed at or frequently visiting battlefield operations centers would attend meetings and receive operations orders, collecting information limited to specific sheets of paper, briefing slides, or notes taken. With the use of distributed computers, networks, and data repositories, commanders today passively share more information with larger audiences. Today, organizations share information with increased expectations for speed (time to disseminate and receive the information), audiences (who can receive the information), and scope (how much information audiences receive.) Looking at the current use of coalition forces in Afghanistan, the distribution of forces has dynamically changed from previous

conflicts such as Operation Desert Storm or World War II. United States and coalition partners routinely collate, intermingle, or task organize their militaries to meet battlefield requirements, necessitating the increased sharing of relevant mission command information such as force allocation, force protection, supply routes, and tracking movement of enemy forces.

To meet this need within Afghanistan for Operation Enduring Freedom, the North Atlantic Treaty Organization (NATO), along with the United States, developed the Afghan Mission Network (AMN). Specifically, this network is designed to "foster collaboration and information sharing by all International Security Assistance Force (ISAF) Troop Contributing Nations (TCN)."[4] In the future, networks like the AMN must overcome challenges related to managing information sharing with coalition partners. These challenges include finding the balance between disclosing enough information to enhance combat operations and protecting against release of information that would jeopardize U.S. and coalition combat operations. To overcome these challenges U.S. policymakers and military commanders must develop, improve, and implement policies, processes, and technology to rapidly and effectively share sensitive mission command information with coalition partners.

This paper begins by reviewing the background of coalition information sharing and introducing the benefits of carefully managed information sharing for both the United States and other nations. Next, this paper examines several ongoing efforts in information sharing, including the AMN currently used in Afghanistan. Using a U.S. Intelligence Community model to assess information sharing, this study reviews the use of the AMN in five critical areas, providing potential explanations and assessment of future risk. Relying on these explanations, this study presents five recommendations to help policymakers support commanders who must balance balancing information sharing with information security requirements.

The Need for Information Sharing

Since the role of the U.S. military is to win the nation's wars, promote national security, and protect national interests, military forces must prepare and train for combat operations. Any large-scale participation of U.S. forces will likely begin with coalition partners, such as participants from NATO. In this type of scenario commanders "will be required to share intelligence with foreign military forces and to coordinate receiving intelligence from those forces."[5] At the national level of government, the United States has published numerous forms of guidance emphasizing the need to share information with coalition partners. The *National Strategic Plan for the War on Terrorism* (4 March 2005) states that "it is important that the United States have the capability to form multinational coalitions…[since] coalitions can contribute significantly to mission accomplishment."[6] The October 2007 *National Strategy for Information Sharing* (NSIS) includes additional guidance: "The exchange of information should be the rule, not the exception, in our efforts to combat the terrorist threat."[7] This NSIS strategy suggests that the United States should work harder to improve information sharing with foreign governments.[8]

The need to share information with coalition partners is balanced by the need to share only appropriate information "with foreign governments to ensure appropriate security and confidentiality of exchanged information."[9] The Congressional Research Service advised Congress to add Networking with Coalition Partners to its list of oversight issues to improve the understanding of benefits and risks associated with coalition information sharing.[10] The U.S. Intelligence Community also published its *Information Sharing Strategy* in February 2008, which identifies a need to manage the risks associated with information disclosure. Sensitive information must be protected but excessive information protection could obscure clues to enemy attacks that might cost lives and potentially endanger the national security of the United States.[11] This document lays out a five-point model for the key questions to ask when considering information sharing. These needs include:

1. Information management (governance)
2. Rules for sharing (policy)

3. Technology to enable sharing and security
4. A culture of sharing
5. Resources to share effectively the information.[12]

This paper adapts the above model to the case of rapidly sharing mission command information within the current coalition of forces in Afghanistan. This paper also provides recommendations to improve the management of information sharing in future operations.

In 1597, Sir Francis Bacon proclaimed that "knowledge is power."[13] Providing leaders with complete situational awareness enhances mission effectiveness and reduces risk of negative consequences to their organizations. This applies to forces inside a coalition as well as adversaries looking to defeat the coalition. Enemy forces who can gain vital information about troop locations, equipment capabilities, readiness, or unguarded avenues of advance, can use this information against coalition forces and change potential overmatch in capability to defeat or stalemate.

The Wikileaks disclosure of U.S. classified tactical military operations in Iraq and Afghanistan offers one example of damaging effects caused by inappropriate disclosure of information. Secretary of Defense Robert Gates stated that the release of the names of cooperative Afghan nationals in these documents are "likely to cause significant harm or damage to the national security interests of the United States."[14] This damage could come from the murder of these supportive Afghan nationals by unsupportive al Qaeda operatives or the destruction of the towns in which these nationals live, where each negative act could degrade ongoing nation building activities in the region.

Within coalitions, the United States shares multiple forms of information with other nations and contributing partners, each with varied levels of nation-to-nation partnering experience and trust. Sharing of information becomes more complex as it is shared outside of an organization with other government agencies, organizations, and then coalition partners.[15] Coalition information sharing begins with communications of administrative matters such as routine electronic mail, which becomes slightly more complicated with inclusion of

attachments that share classified mail. Sharing continues up levels of complexity through common access to information (like databases, file systems, etc.), to current mission command information (like common operational and logistics pictures, unmanned aerial vehicles videos, and ongoing battlefield operations – including artillery missions, aviation strikes, etc.).

Commanders must be aware of the limits of sharing information with coalition partners,[16] and should make informed decisions as to when and what level of information to share with each coalition partner, relying on foreign disclosure officers and international agreements for each nation.[17] Also involved in this balancing act is the assessment of the operational risk of sharing different amounts of information with participating nations, potentially disrupting atmospheres of trust and camaraderie, which could lead to diplomatic issues.[18] Operational risks that are too high in either probability of occurrence or consequence (or both) can degrade the ability of an organization to execute strategy successfully within acceptable impacts to operations.[19]

For the current conflict in Afghanistan, the AMN integrates approximately 45 different nations into a secure information sharing environment to meet the mission command needs of regional military forces. During the year-long process to create this network, the U.S. Central Command (CENTCOM) shifted information that was only previously available through the United States classified network to the coalition network, including critical applications handling warfighter mission areas such as operational environment management, joint fires, joint intelligence and area force protection.[20] For each of these 45 nations, a separate international agreement[21] (or alliance[22]) is in place to identify what information leaders can share in order to remain in compliance with Executive Order 13526, *Classified National Security Information* (January 2010). Within the United States Pacific Command, the command coordinates with up to 39 nations, managing several programs supporting coalition operations, (such as the Combined Communications Interoperability Program) based on individual regional partner security agreements.[23]

Challenges arise when local commanders face new situations, under time constraints such as changes in unit locations which require new

task organizations and partnership. For example, when the United States co-occupies a forward operating base with other nations, other nations may request insight to unmanned aerial video system information or pictures from Persistent Threat Detection System cameras. Although these systems can provide valuable information on enemy troop movements, some international agreements may not include real-time access to these capabilities. A recent example of this issue emerged in South Kandahar, Afghanistan, where 18 nations, including forces from the United States, United Kingdom, Canada and Australia could not see or talk to each other since they were on different secure networks.[24] Other challenges may arise when the co-located, troop-contributing nation does not have equipment that is technologically compatible for information sharing and asks local commanders for use of equipment to ensure a common understanding of the battlefield.[25] Coalition forces must develop both the capability and willingness to securely share and coordinate across organizations to maximize effectiveness in combat.

The Need to Securely Share

As leaders continue to form, modify, disestablish and recreate coalitions to meet mission requirements, the need for international agreements between coalition partners will continue to remain a challenge for policymakers and warfighters. The battlefields of Afghanistan are not the only location where the need for working together as a coalition exists. On December 25, 2009, an al Qaeda operative from Nigeria almost detonated plastic explosives on Northwest Airlines Flight 253, from Schiphol Airport in Amsterdam, Netherlands, to Detroit. The *New York Times* quoted President Barack Obama saying, "This was not a failure to collect intelligence; it was a failure to integrate and understand the intelligence that we already had."[26] The failure was in integrated information on hand by other nations, which was not shared with the United States due to the security concerns. The United States will not continue to allow an atmosphere of status quo and limited information sharing that allows potential terrorist cells to grow stronger.[27]

Guidance from the Department of Defense suggests a need to remove barriers to effective information sharing. This guidance adds a special focus area (#5) to DoD's 2009 Information Sharing Implementation

Plan to reduce improper and over-classification of information, since those actions "undermine the nation's safety and security by impeding timely sharing of perishable information with relative stakeholders, including…coalition partners."[28] The implementation plan also states that currently fielded technologies, processes, governance, and policies are not meeting the needs of combatant commanders for mission partner information sharing. Furthermore, it tasks the Defense Information Systems Agency (DISA) to "[d]evelop an architecture to converge the multiple secret-level coalition networks into a single mission partner assured information sharing environment…"[29]

The creation of international agreements between coalition partners is difficult and time consuming work, which does not support rapid modifications. Even between closest allies, the deliberations between countries can slip from negotiating win-win solutions to the prisoner's dilemma of not cooperating even when it is in the nation's best interest to compromise. The United States may want to limit information sharing to relevant geographic information where the partner nation may want access to theater level readiness information. Conversely, the United States may want unlimited access to sensors managed by a coalition partner, yet the partner may only be willing to share a portion of the data, rather than the information directly from the sensor. International agreements are in place for common coalition partners (such as NATO partners or Australia), but may not be in place in sufficient detail to provide adequate information sharing on local force protection issues for emerging partners (such as other Global Counterterrorism Task Force nations).

Leaders must balance the consistent drive to improve information sharing with equally persistent needs for information security. On a shared battlefield, the United States must trust coalition partners to share information, yet limit the disclosure of information not intended for adversary forces. Although the United States and the European Union have learned the horrors of not sharing information on suspected terrorist personnel and their potential effects on human lives, the duo has "yet to negotiate, draft, and sign a binding international agreement that will govern the sharing of personal information for law enforcement purposes."[30] This leaves both participants open to

additional risk for missing key information and possibly stopping a future terrorist event.

The Department of Defense provides some guidance for commanders in time of war or conflict when there is an immediate need to alter information sharing agreements. The Secretary of Defense delegates to the Chairman of the Joint Chiefs of Staff (CJCS) the authority for "agreements for cooperative or reciprocal operational, logistical, training, or other military support…for agreements concerning operational command of joint forces."[31] The CJCS delegates to overseas unified commanders the authority to negotiate and conclude international military telecommunication agreements with coalition partners when such arrangements are in the national interest.[32] This delegation empowers commanders such as the CENTCOM Commander to negotiate an agreement when needed as coalitions add new partners to the effort. While subordinates generally see empowerment as positive since it allows for faster decision making, there could be long-term consequences if forces share the wrong information (such as equipment capabilities or readiness information of other coalition partner) with a troop contributing nation in the quest to solve operational issues without a true analysis of the strategic importance tradeoffs.

Ongoing Efforts

As technology has improved over the last 20 years, the Department of Defense has continued to improve its capability to share information with coalition partners. Each of these activities generates lessons learned from coalition exercises and operational experiences, which contribute to the development of the best product for the joint warfighter. The AMN currently provides the best baseline to develop future networks to enable secure information sharing.

As the coalition formed in Afghanistan to defeat al Qaeda in support of Operation Enduring Freedom, interoperability concerns required implementation of new processes and agreements to synchronize operations and rapidly share information. In the battle of Marjah, Helmand Province, Afghanistan, a NATO Corps, a British Division, a U.S. Marine Corps Brigade and a U. S. Army Brigade needed to share a common operational picture of the tactical fight.[33] Commanders

can enable such coordination by exchanging liaison officers or loaning radio equipment, but the ongoing coalition demonstrations and today's Network Centric Warfare[34] have led to development of the technical ability to share much more, such as by common operational picture or collaborative planning and discussions. The United States learned some lessons on interoperability from ongoing demonstrations and previous conflicts in Kosovo and Iraq. However, methods such as providing a single U.S. coalition partner (e.g., the United Kingdom), with a combat operations system like U.S. Force XXI Battle Command Brigade and Below (FBCB2) would not be feasible for combat operations in Afghanistan that involve more than 40 coalition partners.

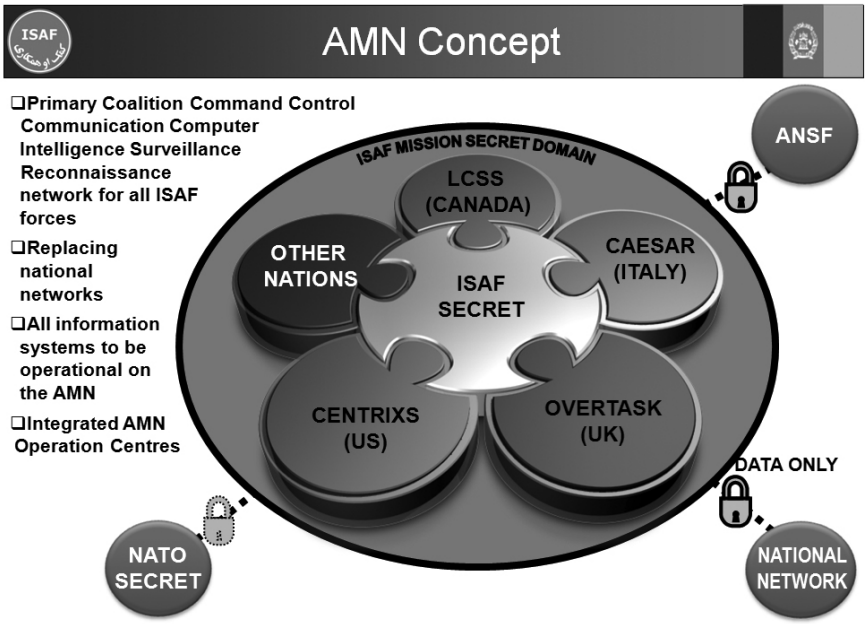

Figure 1. Afghan Mission Network Concept[35]

To meet this interoperability need, the ISAF Commander required a change in culture to normalize a coalition communications network and acquire a capability "to effectively mix United States and Coalition formations within the Regional Command's battle space – down to Company level."[36] The emerging AMN would merge multiple networks and include applications in areas such as intelligence, special operations, NATO, medical, and logistic networks to create the

ability to share the relevant mission command information across the coalition. The network would not necessarily provide new capabilities to forces (e.g., provide automated fire control to forces that still use radio based methods). Instead, it would provide the situational awareness of friendly and enemy force dispositions and locations for critical supplies, thereby providing the ability to better synchronize coalition combat operations. As the system matures over time, it would offer the flexibility to adapt to rapid task organization changes, include additional nations as they join the coalition, and serve as the basis for a network that would operate outside the Afghan theater.

Assessment of Risk

As the United States continues operations in Afghanistan and looks into the future to prepare for future coalition operations, there is a need to assess the risk of whether current coalition mission command efforts are sufficient. Furthermore, if found insufficient, the United States would need to identify areas that should be emphasized in a resource-constrained environment. By adapting the five-point model from the February 2008 U.S. Intelligence Community *Information Sharing Strategy*, the United States could assess the feasibility of the current AMN as a foundation for coalition mission command capability for Operation Enduring Freedom in Afghanistan and for future coalition missions. These assessments lead to specific recommendations to resolve shortcomings and improve future operations.

Consideration 1: Governance

The AMN does have effective governance and leadership to drive effective and secure sharing of information across coalitions. It is important to understand, though, that the question of leadership and governance for the AMN does not begin with the communications and electronics community and a desire more efficiency in passing data. Rather it begins with the need for increased effectiveness.

Technical implementation of the AMN may be in the hands of businessmen and engineers, but leadership of the operational implementation of AMN resides at the senior leadership level in NATO and ISAF/CENTCOM. These senior leaders understand the critical

need for security across the coalition, and they see the AMN as the next phase in implementing a solution across tactical and operational communications between troop contributing nations.

Agencies outside CENTCOM also support the AMN. In DISA, the MNIS Program Management Office is leveraging the success of AMN to create more robust systems for use outside the Afghanistan Theater of Operations. NATO supports the AMN as the "primary Coalition Command Control Communication Computer Intelligence Surveillance Reconnaissance network"[37] for all their contributed forces to ISAF. Additionally, Congress has continued to support financially the initial delivery of the system in the Department of Defense's role to disrupt al Qaeda and the Taliban's use of cyberspace.[38]

There is a low risk of the AMN meeting its governance criteria since this program has tremendous leadership involvement and the stakeholders continue to support the system as it develops additional capabilities. Involved coalition partners see the value of the system and have agreed to the policies required for access, but risk can increase when leaders grant expanded access to networks. In such instances, the ISAF communications section would need to frame the issue for ISAF leadership and try to reach a negotiated agreement that is mainly tied to international agreements

Policies that overstress punishment for exposing too much information, which lead to over-classification of documents, should also be examined. One example is the marking of entire AMN briefings as "NOFORN" (Not Releasable to Foreign Nationals), when only one slide may be unsuitable for release outside U.S. forces. Furthermore, since the AMN program requires additional funding to achieve a full operational capability, there is increased risk that leaders may withdraw support and invest in other capabilities.

Consideration 2: Policy

Policies and standards are not sufficient to guide the balance of sharing information with the security concerns. This is the area of greatest concern for the future of the AMN and other efforts. Current policies nested in various U.S. government strategy documents (e.g., the *National*

Strategy for Information Sharing or the Information Sharing Strategy) and Department of Defense publications (e.g., the DoD Plan or Joint Publication 2-0 on Joint Intelligence) do not provide enough detail on the balance between security and information sharing. In general, these documents explain how to remove barriers and increase sharing with coalition partners, giving the combatant commander responsibility for rapidly analyzing and deciding how much information to share in the gap created between the international agreements.

Unfortunately, the time it takes to broker international agreements cannot match the fast-flowing changes in both technology and task organization on the battlefield. In addition, combatant commanders may err on the side of overcoming operational issues and winning tactical battles, without sufficient analysis of the second-order effects of strategic decisions.

For example, U.S. and coalition forces must agree on sharing video feeds in order to overcome the advance of enemy forces. If a coalition partner does not have adequate protection from hackers or from internal misuse of classified material, such video could reveal U.S. capabilities to enemy forces, allowing the enemy to adapt and thereby reducing the U.S. and coalition tactical advantage. Although the AMN's architecture requires a conscious decision to tag and post information to the shared data environment, the lack of guidance to prevent potential compromises of shared information could hinder future operations. Current guidance assumes adequate time to initiate coalition based networks, which is based on the obsolete idea of a Cold War or Desert Storm buildup phase to operations, rather than rapid transitions in contemporary operations from Phase Zero Shaping Operations to Phase III Dominate (Combat Operations).[39]

Even with significant advances in technology, there is a high probability that operators will improperly share information across a coalition network, and there is likely a moderate negative consequence based on the shared information. Brigadier General Susan Lawrence, while she was commander of the U.S. Army Network Enterprise Technology Command/9th Signal Command, stated that According to one former U.S. Army commander, "Our enemies are all over the network."[40] Although this observation focused on a garrison-based

network, it applies to all U.S. combat networks. Without additional policy guidance to address the rapid creation of coalition networks, commanders will continue to face elevated risk when pressed with sharing classified information with coalition partners.

Consideration 3: Technology

Technology is in place to enable effective and secure sharing across the coalition. This is a major strength of the AMN. Multiple Army Acquisition organizations came together and took the best ideas from the multiple coalition information sharing systems across to work with NATO to develop the AMN.[41] The system provides the common core ISAF Secret network that participating coalition partners can securely tie into the network interconnection points without fear of undue exposure to host nation systems, such as the U.S. Combined Enterprise Regional Information Exchange System (CENTRIXS). Common data standards help participants to organize, indentify, and search for information. Participants can push information to the core domain and pull information from other participating sources. Administrated control access to the network through country-based user interfaces and country network administrators can audit system usage to ensure only valid participants access the core, without infringing into the sovereignty of the coalition partners host system.

Although the ISAF Secret network provides the screening at the nation level, the limit of not automating control at the user level could lead to security concerns due to a perceived lack of individual accountability. There is a low to moderate risk of individuals violating security protocols and revealing information to unauthorized viewers. However, this risk can increase as technical measures are developed to avoid security protocols.

Unsecure networks hosted on the World Wide Web are more susceptible to hackers and data loss. This network begins with a secret framework that carries with it a general expectation of trusted viewers. The risk becomes more moderate as coalition partners become interested in data about other troop contributing nations, specifically nations that may be adversaries or unfriendly outside the Afghanistan theater.

Other technology risks include the rapid need to modify sharing permissions with coalition partners based on short-term tactical needs, such as short-term access to unmanned aerial vehicle (UAV) video, without truly assessing the cost of acknowledging such capabilities to the partner coalition troop contributing nation. For example, sharing video from a high altitude UAV to synchronize effort and counter an imminent threat could expose the capability of such UAVs to operate in the local conditions. The ability for information sharing across multiple languages requires further development. In addition, there always remains a minor risk that a network user may place on the network misleading data (e.g., a position or weather estimate rather than precise data). This may lead another user to mistakenly make an incorrect decision based on that data.

Consideration 4: Culture

The culture of coalition mission command information users often detracts from securely sharing information across the network. This area is improving but is not fully developed. Certainly the U.S. Armed Forces have learned from the lessons of Desert Storm and Kosovo the need to share information and have made great progress in the area. However, the equipment to ensure sharing is still insufficient. The 21st century technology involved with Network Centric Warfare has developed the ability to share much more than voice commands or paper files among liaison officers. The involvement of ISAF and CENTCOM leadership has helped promote a culture of sharing over the almost 10 years of conflict in Afghanistan. This motivates users to share data across the network, recognizing the synergetic value of pooling information on known or suspected enemy locations to enable more productive attacks or tie together information on terrorists to locate hideouts and leader locations. The authority to decide what information to place on the core ISAF network remains at the originating source. However routine coalition communication meetings and training enable participants to voice concerns over insufficient sharing arrangements. Additionally, the global impact of unauthorized document release from Wikileaks may prompt organizations to revert to more restrictive cultures that share less information.

The will to share will increase as partners continue to work together, reducing the risk of cultural barriers impeding coalition information sharing. Over the past decade, ISAF partners have overcome many cultural barriers, thus allowing the emergence of new technology that enables faster downloads of information and increased bandwidth for sharing graphics and video. There will also remain the risk of counterintelligence, which leaders must consider in coalition operations.

Consideration 5: Economics

There are sufficient resources to enable secure information sharing. With the United States investing approximately $100 million and NATO investing an additional $15 million to improve the ISAF Secret Network,[42] there have been sufficient resources infused into the AMN to provide a base for information sharing. Over time, multiple programs have invested additional resources to ensure that data can traverse the AMN, which may include rewriting software code to enable sharing outside the U.S. CENTRIXS.

Although NATO and the United States adequately funded the initial capability of the AMN, there remains an annual funding requirement for ongoing operations and maintenance that competes each year with other budget priorities. Also, as commanders deem information sharing more valuable, there is a moderate risk that system users will want enhanced capabilities, such as additional bandwidth or faster download speeds. This will require additional investments. This risk is greater for the United States, which has a larger leadership role in ISAF than other nations. However, there will continue to be shared responsibility for each troop-contributing nation to improve their user terminals to accept the information provided over the AMN. User training time is but one resource that will continue to present challenges. As new coalition partners join the AMN, leaders and policymakers must simplify processes involved with joining the AMN, training users of the systems on how to organize and search for information, and finding ways to push information to other AMN participants.

Recommendations

Based on the five considerations derived from the U.S. Intelligence Community model, participants in the information sharing community can improve each area of governance, policy, technology, culture, and economics. Through a combination of improvements in technology and guidance, the U.S. government can enhance the AMN and future coalition networks and equip them to better share information across the coalition while maintaining the security protocols that are required to protect national security.

Recommendation 1: Governance. To ensure the AMN retains effective governance and leadership to drive effective and secure sharing of information across coalitions, CENTCOM and ISAF leaders must continue strategic communication with network participants. This consistency becomes increasingly relevant as military leaders of organizations change over time more frequently than civilian counterparts. The DISA should continue to provide updates through CENTCOM on the transition from a product focused on Afghanistan to a more deployable system, able for rapid installation regardless of theater of operation The ISAF should continually seek feedback from coalition partners about future developmental needs and document changes required to convert tactical expediency of battlefield operations into international agreements. As long as the United States and organizations like NATO work together and cooperate rather than compete for the leadership role in this effort, the AMN can continue to provide effective information sharing across the coalition.

Recommendation 2: Policy. Policymakers should address the commanders' need for rapid decision-making regarding information sharing and potential effects. The revision of Department of Defense Directive 8320.2 should include guidance on levels of information sharing based on time constraints, current theater operations, and future tactical confrontations. Joint Publication 6-0 (Joint Communications) should expand the guidance provided to foreign disclosure officers on tiered level of information releasability that is situational dependant rather than an "all or nothing" approach. The DoD Information Sharing Implementation Plan and Joint Publication 2-0 (Joint Intelligence) should include additional guidance to help

commanders make rapid information sharing decisions in situations like forming new task organizations in forward operating basis or adding new coalition partners to emerging combat operations.

If possible, nations should craft international agreements giving maximum flexibility to commanders, stressing only the limits of what not to share (e.g., key technologies, peer capabilities) rather than prescribe what information can be shared (e.g., common terrain products, electronic mail). Although policy changes alone will not improve information sharing, they provide the foundation for improved decision making for commanders faced with balancing information security and sharing requirements. This recommendation takes into account the danger that overly detailed policy restricts the ability of commanders to make flexible decisions on the battlefield to overcome emerging challenges. Therefore, policymakers must not impose limits on commanders beyond those contained in laws or statutes.

Recommendation 3: Technology. The CENTCOM and ISAF should continue periodic infusion of well-tested technology to incrementally improve secure information sharing across the coalition. Upgrades in both the software that manages sharing permission and the training of coalition partners on the use of the AMN can continue to improve the technologies ability to balance security and information sharing. Future integration of language independence or easily translated software can help coalition partners better understand the mission command information. In addition, the software requires improvements in technology to counter emerging threats from future hackers, who may capture or decrypt weaker coalition partner security systems. Continue to enhance the ability of the coalition network to handle additional data and information bandwidth, and integrate advances in communications technologies to improve system reliability and user interfaces. The Department of Defense should continue to manage efforts to develop and field additional capability as acquisition programs of record, to ensure adequate testing of security and interoperability. In parallel, additional capability will require additional training, which the U.S. Army should integrate into initial entry and follow on courses taken at Training and Doctrine Command schools.

Recommendation 4: Culture. Continue to stress the importance of coalitions, cultural awareness, and trust among coalition partners. Encourage coalition partners to continue to populate shared environments with relevant information. Overcome the chilling effect negative media coverage related to inadvertent or unauthorized release of information (e.g., Wikileaks) and celebrate successes in sharing information that lead to battlefield victories.

Recommendation 5: Economics. Promote awareness of successes in the AMN among key stakeholders, including include Congress and Department of Defense leadership, to ensure continued funding in maintenance of current systems and development of future systems. Invest as soon as possible for the next generation of the AMN, developing it into a system that incorporates other coalition lessons learned from the USEUCOM Battlefield Information Collection and Exploitation Systems program and the variant of the Global Command and Control System used in Korea.

Re-evaluate the need for multiple versions of coalition information sharing systems focused on geographic areas, and develop one modular system capable of integration of any coalition partner regardless of hardware. Understanding systems may require minor adjustments to hardware, but open systems architecture and non-proprietary software will reduce rework needed for future coalition partners to join United States involved networks.

Realize that as NATO and the United States reduces its involvement in the coalition in Afghanistan, Congress and other financial organizations may reduce funding from Defense spending to other national needs. To prepare for follow-on conflicts, acquisition organizations should pool resources and work together to continue to improve on the AMN foundation and reduce the network construction time for follow-on operations. Acquisition program managers and writers of system requirements should anticipate the need to modify ongoing and future systems to allow for better integration into coalition networks.

Conclusion

While policymakers and commanders adequately balance information sharing and security each day through their dedicated intelligence, communications, and foreign disclosure officers, improvements to published guidance and technology can reduce risk and preserve U.S. combat advantages. As President Barack Obama states in the Introduction of the 2010 National Security Strategy, throughout history the United States has operated with coalition partners to win World War II and end the Cold War; and, in the future, the United States will continue to strengthen coalition alliances to achieve national objectives.[43] The Department of Defense has several ongoing efforts in information sharing, highlighted by the success of the AMN in Operation Enduring Freedom. Although the AMN provides a significant improvement over historical methods of coalition information sharing, and has significant leadership support for the process and culture of sharing, the Department of Defense still needs to revise existing guidance to support the rapid requirements of combatant commanders. With adequate funding, technology can resolve ongoing issues, but follow-on conflicts may not allow the eight-year learning curve seen in Afghanistan to ensure coalition partners can securely share information at the start of operations.


U.S. ARMY WAR COLLEGE
Prudens
Futuri
Carlisle Barracks, PA

Endnotes

Preface

1. Reagan, Ronald. *National Security Decision Directive 130*. Washington, D.C.: The White House, 6 March 1984. Available from http://www.fas.org/irp/offdocs/nsdd/nsdd-130.htm (accessed December 9, 2011.)
2. Neilson, Robert E. and Daniel T. Kuehl, "Evolutionary Change in Revolutionary Times: A Case for a New National Security Education Program," *National Security Strategy Quarterly* (Autumn 1999): 40.

Section One: Information Effects in the Cyberspace Domain

Introduction

1. Leon E. Panetta, *Department of Defense Strategy for Operating in Cyberspace* (Washington, DC: U.S. Department of Defense, July 2011), 1.

Securing Cyberspace: Approaches to Developing an Effective Cybersecurity Strategy

1. Stuart Starr, "Toward a Preliminary Theory of Cyberpower," in *Cyberpower and National Security*, ed. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (Washington, DC: Potomac Books and National Defense University Press, 2009), 51-52.
2. Barack H. Obama, *National Security Strategy* (Washington, DC: The White House, May, 2010), 27.
3. Robert M. Gates, *Quadrennial Defense Review Report* (Washington, DC: Department of Defense, February, 2010), 37.
4. Obama, *National Security Strategy*, 27.
5. Daniel T. Kuehl, "From Cyberspace to Cyberpower: Defining the Problem," in *Cyberpower and National Security*, ed. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (Washington, DC: Potomac Books and National Defense University Press, 2009), 24. Dr. Kuehl cites the William Gibson science fiction novel, *Neuromancer*.
6. U.S. Joint Chiefs of Staff, *Department of Defense Dictionary of Military and Associated Terms*, Joint Publication 1-02 (Washington, DC: U.S. Joint Chiefs of Staff, November 8, 2010, amended through January 31, 2011), 92.
7. Kuehl, "From Cyberspace to Cyberpower," 28. A similar definition is found in U.S. Joint Chiefs of Staff, *Joint Operations*, Joint Publication 3-0 (Washington,

DC: U.S. Joint Chiefs of Staff, September 17, 2006, incorporating Change 2, March 22, 2010), II-22.

8. Ibid., 38.
9. William Oliver Stevens and Allan Westcott, *A History of Sea Power* (New York: Doubleday, 1920), 443, quoted in Kuehl, "From Cyberspace to Cyberpower: Defining the Problem," 38.
10. National Research Council of the National Academies, *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities* (Washington, DC: The National Academies Press, 2009), 10-11.
11. Ibid., 80-81.
12. CBS News/Associated Press, "Lights Back On In Brazil After Blackout," November 11, 2009, http://www.cbsnews.com/stories/2009/11/10/world/main5607148.shtml?tag=mncol;lst;1 (accessed February 27, 2011).
13. Jeffrey Carr, *Inside Cyber Warfare* (Sebastopol, CA: O'Reilly Media, 2010), 3.
14. Timothy L. Thomas, "Nation-state Cyber Strategies: Examples from China and Russia," in *Cyberpower and National Security*, ed. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (Washington, DC: Potomac Books and National Defense University Press, 2009), 475-476.
15. Clay Wilson, "Cyber Crime," in *Cyberpower and National Security*, ed. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (Washington, DC: Potomac Books and National Defense University Press, 2009), 420.
16. U.S. Congress, House of Representatives, Committee on Armed Services, *U.S. Cyber Command: Organizing for Cyberspace Operations*, 111th Congress, hearing held September 23, 2010 (Washington, DC: U.S. Government Printing Office, 2010), 37.
17. Carr, *Inside Cyber Warfare*, 12-13.
18. Ibid., 11.
19. Ibid., 4.
20. Kuehl, "From Cyberspace to Cyberpower," 39.
21. Harold Kwalwasser, "Internet Governance," in *Cyberpower and National Security*, ed. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (Washington, DC: Potomac Books and National Defense University Press, 2009), 498.
22. Starr, "Toward a Preliminary Theory of Cyberpower," 67.
23. Ibid., 67.
24. Franklin D. Kramer, "Cyberpower and National Security: Policy Recommendations for a Strategic Framework," in *Cyberpower and National Security*, ed. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (Washington, DC: Potomac Books and National Defense University Press, 2009), 7.

25. U.S. Air Force, "Cyber Command Achieves Full Operational Capability," release number 031110, November 3, 2010, http://www.afspc.af.mil/pressreleasearchive/story.asp?id=123229293 (accessed April 21, 2011).
26. U.S. Strategic Command, "Factsheet: U.S. Cyber Command," http://www.stratcom.mil/factsheets/Cyber_Command (accessed April 18, 2011).
27. William J. Lynn, III, "Remarks at STRATCOM Cyber Symposium," May 26, 2010, http://www.defense.gov/Speeches/Speech.aspx?Speechid=1477 (accessed April 18, 2011).
28. Ibid.
29. Cheryl Pellerin, "Lynn: Cyberspace is the New Domain of Warfare," (Washington, DC: American Forces Press Services, October 18, 2010), http://www.defense.gov/news/newsarticle.aspx?ID=61310 (accessed November 20, 2010).
30. U.S. Congress, *U.S. Cyber Command*, 40.
31. National Security Council, *The Comprehensive National Cybersecurity Initiative*, http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative (accessed April 18, 2011).
32. Lynn, "Remarks at STRATCOM Cyber Symposium."
33. Ibid.
34. Department of Homeland Security, "Privacy Impact Assessment for the Initiative Three Exercise," March 18, 2010, (Washington DC: Department of Homeland Security, 2010): 3.
35. The White House, "National Cybersecurity Center Policy Capture," http://www.whitehouse.gov/files/documents/cyber/CybersecurityCentersGraphic.pdf (accessed April 21, 2011).
36. Shaun Waterman, "U.S. Cybersecurity Head Quits, Citing Growing Role of Spy Agencies," (Washington DC: UPI, March 11, 2009), http://www.upi.com/Top_News/Special/2009/03/11/US-cybersecurity-head-quits-citing-growing-role-of-spy-agencies/UPI-64411236692969/ (accessed April 21, 2011).
37. Director Beckstrom argued that improved checks and balances would result by keeping the operational agencies separate, a policy contrary to the principle of unity of effort. Though he could have, he did not advocate for legislative or judicial oversight, similar to Congressional oversight of the military or of the intelligence community. Legislative or Judicial oversight would provide effective checks and balances while maintaining the benefits of interagency collaboration and cooperation.
38. National Research Council of the National Academies, *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*, 67.
39. Ibid.

40. Carr, *Inside Cyber Warfare*, 34-35.
41. International Criminal Police Organization, "About INTERPOL," http://www.interpol.int/public/icpo/default.asp (accessed April 25, 2011).
42. Carr, *Inside Cyber Warfare*, 35.
43. Ibid., 15-17.
44. Kwalwasser, "Internet Governance," 517.
45. Council of Europe, *Convention on Cybercrime*, European Treaty Series No. 185 (Budapest: November 23, 2001).
46. Carr, *Inside Cyber Warfare*, 67.
47. Obama, *National Security Strategy*, 27.
48. U.S. Joint Chiefs of Staff, *Deterrence Operations Joint Operations Concept* (Washington, DC: U.S. Joint Chiefs of Staff, December 2006), 20.
49. National Research Council of the National Academies, *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*, 303.
50. Richard L. Kugler, "Deterrence of Cyber Attacks," in *Cyberpower and National Security*, ed. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (Washington, DC: Potomac Books and National Defense University Press, 2009), 314.
51. National Research Council of the National Academies, *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilitie*s, 141.
52. U.S. Congress, *U.S. Cyber Command*, 40.
53. Kramer, "Cyberpower and National Security," 19.
54. National Research Council of the National Academies, *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*, 309.
55. Ibid., 312.
56. Carr, *Inside Cyber Warfare*, 179-182.
57. Ibid., 181.
58. Ibid., 182.
59. Ibid.
60. National Research Council of the National Academies, *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*, 310.
61. Carr, *Inside Cyber Warfare*, 15-17.
62. National Research Council of the National Academies, *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilitie*s, 312.
63. Carr, *Inside Cyber Warfare*, 79-83.

A Strategic Approach to Network Defense: Framing the Cloud

1. Vivek Kundra, *25 Point Implementation Plan to Reform Federal Information Technology Management* (Washington, DC: The White House, December 9, 2010): 5.
2. Clive Davidson, "Cloud Control," *Risk* 23, no. 10 (October 2010) in ProQuest (accessed November 22, 2010): 70.
3. Ibid., 71.
4. Kundra, *25 Point Implementation Plan to Reform Federal Information Technology Management*, 5.
5. Ibid., 5.
6. U.S. Department of the Defense, *Dictionary of Military and Associated Terms, Joint Publication 1-02, (Washington, DC: U.S. Department of the Defense, April 12, 2001 amended through September 30, 2010), 126.*
7. *William T. Lord,* "Cyberspace Operations: Air Force Space Command Takes the Lead," *High Frontier* 5, no. 3 (May 2009): 3.
8. Intel, "Moore's Law," (Santa Clara, CA: Intel Corporation, 2010), http://www.intel.com/ technology/mooreslaw/ (accessed November 19, 2010).
9. Arthur K. Cebrowski, "Transformation and the Changing Character of War?," *Transformation Trends,* June 17, 2004, http://www.oft.osd.mil/library/library_files/trends_370_Transformation%20Trends-17%20June%202004%20Issue.pdf (accessed January 5, 2011).
10. *C*had Perrin, *The CIA Triad* (Louisville, KY: TechRepublic, June 30, 2008), http://www.techrepublic.com/blog/security/the-cia-triad/488 (accessed January 23, 2011).
11. Cisco Learning Network, "What is the CIA Triad," https://learningnetwork.cisco.com/message/59995 (accessed November 19, 2010).
12. Perrin, *The CIA Triad.*
13. U.S. Department of the Defense, Information Assurance, DOD Directive 8500.01E (Washington, DC: U.S. Department of the Army, October 24, 2002, certified current April 23, 2007), 4.
14. U.S. Department of the Army, *Information Assurance*, Army Regulation 25-2, (Washington, DC: U.S. Department of the Army, March 23, 2009): 1.
15. U.S. Department of the Defense, *Dictionary of Military and Associated Terms,* Joint Publication 1-02, 175.
16. David M. Hollis, "USCYBERCOM: The Need for a Combatant Command versus a Subunified Command," *Joint Force Quarterly*, no. 58 (Third Quarter 2010): 49.

17. Jeffrey L. Caton, "Cyberspace and Cyber Operations," *Information Operations Primer,* AY11 ed. (Carlisle Barracks, PA: U.S. Army War College, November 2010), 21.
18. *National Academy of Engineering*, "Securing the Electricity Grid," http://www.nae.edu/ Publications/Bridge/TheElectricityGrid/18868.aspx (accessed January 3, 2011).
19. Caton, "Cyberspace and Cyber Operations," 20.
20. National Academy of Engineering, "Securing the Electricity Grid."
21. McAfee, "In the Crossfire: Critical Infrastructure in the Age of Cyber War" (Santa Clara, CA: McAfee, 2011), 10, http://newsroom.mcafee.com/images/10039/In%20the%20Crossfire_CIP% 20report.pdf (accessed January 26, 2011).
22. Ibid., 9.
23. Andrew Hildick-Smith, "Security for Critical Infrastructure SCADA Systems," *SANS Institute InfoSec Reading Room* (Bethesda, MD: SANS Institute, February 23, 2005), 5, www.sans.org/reading_room/whitepapers/warfare/security-critical-infrastructure-scada-systems_1644 (accessed November 19, 2010).
24. George W. Bush, *Presidential Executive Order 13286 amending 13231 Critical Information Protection in the Information Age* (Washington, DC: The White House, February 28, 2003).
25. Hildick-Smith, "Security for Critical Infrastructure SCADA Systems," 5.
26. Timothy Shimeall, "Countering Cyber War," *NATO Review* 49, no. 4 (Winter 2001): 17.
27. U.S. Computer Emergency Readiness Team, "Cyber Threat Source Descriptions," http://www.us-cert.gov/control_systems/csthreats.html (accessed January 3, 2011).
28. Ibid.
29. Ibid.
30. Ibid.
31. Ibid.
32. Ibid.
33. Ibid.
34. Ibid.
35. Ibid.
36. Symantec "Intelligence Quarterly Report for July–September 2010" (Mountain View, CA: Symantec, 2010), 6, http://www.symantec.com/content/en/us/enterprise/white_papers/b-symc_intelligence_qtrly_july_to_sept_WP_21157366.en-us.pdf (accessed December 15, 2010).

37. Ibid., 6.
38. Brian M. Mazanec, "The Art of Cyber War," *Journal of International Security Affairs*, no. 16 (Spring 2009): 84.
39. Shimeall, "*Countering Cyber War,"* 16.
40. Dennis C. Blair, *Annual Threat Assessment of the Intelligence Community for the Senate Select Committee on Intelligence* (Washington, DC: U.S. Senate, February 2, 2010), 4.
41. Ibid., 40.
42. U.S. Department of Homeland Security, *Recommended Practice: Improving Industrial Control Systems Cybersecurity with Defense-In-Depth Strategies* (Washington, DC: U.S. Department of Homeland Security, October 2009): 14.
43. Unsecured Economies: Protecting Vital Information (Santa Clara: McAfee, 2009), 3, http://resources.mcafee.com/content/NAUnsecuredEconomiesReport (accessed January 8, 2011).
44. Ibid.
45. U.S. Department of Homeland Security, *Recommended Practice: Improving Industrial Control Systems Cybersecurity with Defense-In-Depth Strategies,* 14.
46. *Unsecured Economies: Protecting Vital Information, 7.*
47. Ibid.
48. Elinor Mills, "Cloud Computing Security Forecast: Clear Skies," *CNET News,* January 27, 2009, http://news.cnet.com/8301-1009_3-10150569-83.html (accessed January 26, 2011).
49. Ibid.
50. Hollis, "USCYBERCOM: The Need for a Combatant Command versus a Subunified Command," 49.
51. Davidson, "Cloud Control," 72.
52. Ibid., 73.
53. Kundra, *25 Point Implementation Plan to Reform Federal Information Technology Management*, 7.
54. Ibid.
55. Ibid.
56. Ibid., 8.
57. U.S. Department of Homeland Security, *Recommended Practice: Improving Industrial Control Systems Cybersecurity with Defense-In-Depth Strategies,* 14.
58. Ibid., 15.
59. Ibid.

60. Kundra, *25 Point Implementation Plan to Reform Federal Information Technology Management*, 6.
61. Ibid.
62. U.S. Department of Homeland Security, *Recommended Practice: Improving Industrial Control Systems Cybersecurity with Defense-In-Depth Strategies,* 29.
63. David Binning, "Top Five Cloud Computing Security Issues," *Computer Weekly.com*, April 2, 2009, http://www.computerweekly.com/Articles /2010 /01/12/235782/Top-five-cloud-computing-security-issues.htm (accessed January 9, 2011).
64. Ibid.
65. Robert M. Gates, *Submitted Statement to Senate Armed Services Committee* (Washington, DC: U.S. Senate, January 27, 2009), 8.
66. U.S. Office of Management and Budget, "IT Dashboard," http://it.usaspending.gov/ (accessed January 27, 2011).
67. Ibid.
68. Ibid.
69. Kundra, *25 Point Implementation Plan to Reform Federal Information Technology Management*, 3.
70. Ibid.
71. Ibid., 1.
72. J. Nicholas Hoover, "NSA Details Information Assurance Spending," *InformationWeek*, April 9, 2010, http://www.informationweek.com/news/government/security/showArticle.jhtml?articleID=224202447 (accessed January 27, 2011).
73. Kundra, *25 Point Implementation Plan to Reform Federal Information Technology Management*, 1.
74. U.S. Joint Forces Command, *Joint Operating Environment* (Norfolk, VA: U.S. Joint Forces Command, February 18, 2010), 34.
75. U.S. Department of Commerce, *Safe Harbor Overview* (Washington, DC: U.S. Department of Commerce, 2000), http://www.export.gov/safeharbor/eg_main_018236.asp (accessed January 10, 2010).
76. Ibid.
77. World Privacy Forum, "The US Department of Commerce and International Privacy Activities: Indifference and Neglect," November 22, 2010, http://www.worldprivacyforum.org/pdf/USDepartmentofCommerceReportfs.pdf (accessed January 10, 2011), 19.
78. U.S. Joint Forces Command, *Joint Operating Environment, 36.*
79. Ibid.

80. Gregory C. Wilshusen, *Testimony Before the Subcommittee on Government Management, Organization, and Procurement, Committee on Oversight and Government Reform*, U.S. House of Representatives (Washington, DC: U.S. Congress), March 24, 2010), 11.

81. Ibid., 5.

82. U.S. Joint Forces Command, *Joint Operating Environment, 36.*

83. Shimeall, "Countering Cyber War," 18.

84. Carl von Clausewitz, *On War*, trans. Michael Howard and Peter Paret (Princeton, NJ: Princeton University Press, 1989), 364.

Crime or War: Cyberspace Law and its Application for Intelligence

1. U.S. Deputy Secretary of Defense Gordon England, "The Definition of Cyberspace," memorandum for Secretaries of the Military Departments, Washington, DC, May 12, 2008, 1; Melissa Hathaway, *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure* (Washington, DC: U.S. Executive Office of the President, 2009), 1; U.S. Joint Chiefs of Staff, *Department of Defense Dictionary of Military and Associated Terms*, Joint Publication 1-02 (Washington, DC: U.S. Joint Chiefs of Staff, November 8, 2010), 86. This paper uses the joint definition of cyberspace cited in these three sources. However, there are at least 15 different definitions of cyberspace discussed in Daniel T. Kuehl, "From Cyberspace to Cyberpower: Defining the Problem," in *Cyberpower and National Security*, ed. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (Washington, DC: National Defense University Press, 2009), 26-28.

2. George W. Bush, *The National Strategy to Secure Cyberspac*e (Washington, DC: The White House, February 2003), 1; Barack Obama, *Remarks by the President on Securing the Nation's Cyber Infrastructure* (Washington, DC: The White House, May 29, 2009), 1.

3. George W. Bush, *National Strategy to Secure Cyberspace*, 2; Hathaway, Cyberspace Policy Review, 1; Dennis C. Blair, *National Intelligence Strategy* (Washington, DC: Office of the Director of National Intelligence, August 2009), 9; Richard A. Clarke and Robert K. Knake, *Cyber War: The Next Threat to National Security and What To Do About It* (New York, NY: Harper Collins Publishers, 2010), 145-146; Lolita C. Baldor, "General Suggests 'Secure Zone' to Counter Cyber Threats," *Fayetteville Observer*, September 24, 2010. According to Clarke and Knake, "of the eighteen civilian infrastructure sectors identified as critical by the Department of Homeland Security, all have grown reliant on the Internet to carry out their basic functions, and all are vulnerable to cyber-attacks by nation-state actors." These sources also agree that the majority of national infrastructure is privately owned and operated. Baldor states that 85% of national infrastructure is owned and operated by private companies. Private ownership makes it subject to less federal regulation and control than government

networks that fall under the Federal Information Security Management Act. According to the National Intelligence Strategy, "the architecture of the Nation's digital infrastructure, based largely upon the Internet, is neither secure nor resilient." Military cyber-exercises like *Eligible Receiver* and homeland security cyber-exercises like *Cyber Storm* have specifically identified multiple vulnerabilities in critical infrastructure networks. For more on these exercises and network vulnerabilities see Bradley K. Ashley, *Anatomy of Cyberterrorism: Is America Vulnerable?* (Maxwell Air Force Base, AL: U.S. Air War College, 2003), 25-26; Scott Beidleman, *Defining and Deterring Cyber War*, Strategy Research Project (Carlisle Barracks, PA: U.S. Army War College, 2009), 3; Thomas C. Wingfield, *The Law of Information Conflict: National Security Law in Cyberspace* (Falls Church, VA: Aegis Research Corporation, 2000), 22; and U.S. Department of Homeland Security, National Cyber Security Division, *Cyber Storm Exercise Report* (Washington, DC: U.S. Department of Homeland Security, National Cyber Security Division, September 12, 2006), 1-20.

4. U.S. Joint Chiefs of Staff, *DoD Dictionary of Military and Associated Terms*, 67.

5. Ibid. A simpler, but less comprehensive, definition used by Martin Libicki, is when "states steal data from other states," but I would add non-state actors as potential thieves as well. See Martin C. Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica, CA: RAND, 2009), 14.

6. Ibid., 68. Again, a simpler, less comprehensive definition, used by Martin Libicki, is "deliberate disruption or corruption by one state of a system of interest to another state," but I would also add non-state actors as potential attackers as well. See Libicki, *Cyberdeterrence and Cyberwar*, 23.

7. Clay Wilson, *Information Operations and Cyberwar: Capabilities and Related Policy Issues* (Washington, DC: U.S. Library of Congress, Congressional Research Service, September 14, 2006), 5.

8. Thom Shanker, "Cyberwar Chief Calls for Secure Computer Network," *New York Times*, September 23, 2010.

9. Beidleman, *Defining and Deterring Cyber War*, 2 and 15-16.

10. Wingfield, *Law of Information Conflict*, 5.

11. Ibid., xvi.

12. Duncan B. Hollis, "Why States Need an International Law for Information Operations," *Lewis & Clark Law Review* 11, no. 4 (Winter 2007): 1023-24; Jeffrey T. G. Kelsey, "Hacking Into International Humanitarian Law: The Principles of Distinction and Neutrality in the Age of Cyber Warfare," *Michigan Law Review* 106, no. 7 (May 2008): 1430; Paul A. Matus, *Strategic Impact of Cyber Warfare Rules for the United States*, Strategy Research Project (Carlisle Barracks, PA: U.S. Army War College, 2010), 14-15.

13. Wingfield, *Law of Information Conflict*, 73.

14. Ibid., 39; United Nations, "Charter of the United Nations," http://www.un.org/en/documents/charter/index.shtml (accessed December 7, 2010). "All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations."

15. Ibid., 123.

16. Ibid., 39-40. "Nothing in the present Charter shall impair the inherent right of individual or collective self-defense if an armed attack occurs against a Member of the United Nations, until the Security Council has taken the measures necessary to maintain international peace and security."

17. Ibid., 123.

18. Ibid., 111; Bruno Simma, *The Charter of the United Nations: A Commentary* (Oxford, UK: Oxford University Press, 1994), 670; United Nations, "United Nations General Assembly Resolution 3314," http://www.un.org/ga/search/view_doc.asp?symbol=A/RES/3314(XXIX) (accessed December 7, 2010). Some examples include: invasion, bombardment and cross-border shooting; blockade; attack on the land, sea, or air forces or on the civilian marine and air fleets; breach of stationing agreements; placing territory at another state's disposal; and participation in the use of force by militarily organized unofficial groups.

19. International Committee of the Red Cross, "The Geneva Conventions of 12 August 1949," http://www.icrc.org/ihl.nsf/INTRO/365?OpenDocument (accessed December 7, 2010). The exact wording is: "Armed conflict exists upon: declaration of war; occurrence of any other armed conflict between two or more contracting parties even if state of war is not recognized by one of them; and in all cases of partial or total occupation even if met with no armed resistance."

20. Walter G. Sharp, Sr., *Cyber Space and the Use of Force* (Falls Church, VA: Aegis Research Corporation, 1999), 69.

21. Graham H. Todd, "Armed Attack in Cyberspace: Deterring Asymmetric Warfare with an Asymmetric Definition," *The Air Force Law Review*, vol. 64 (2009): 71.

22. Sharp, *Cyber Space and Use of Force*, 69. According to Sharp, "what constitutes a use of force of a scope, duration, and intensity that constitutes an armed attack and triggers the law of armed conflict is a question of fact that must be subjectively analyzed in each and every case in the context of all relevant law and circumstances."

23. Wingfield, *Law of Information Conflict*, 113.

24. Michael N. Schmitt, *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework* (Colorado Springs, CO: Institute of Information Technology Application, 1999), 18-19; Libicki, *Cyberdeterrence and Cyberwar*, 179-180. A good example of applying the Schmitt framework to the 2007 CNA against Estonia is in Thomas C. Wingfield, "International

Law and Information Operations," in *Cyberpower and National Security*, ed. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (Washington, DC: National Defense University Press, 2009), 527-533.

25. Wingfield, *Law of Information Conflict*, 100-101; Matus, *Strategic Impact of Cyber Warfare Rules*, 12; Stephen W. Korns and Joshua E. Kastenberg, "Georgia's Cyber Left Hook," *Parameters* 38, no. 4 (Winter 2008-09): 60; Arie J. Schapp, "Cyber Warfare Operations: Development and Use Under International Law," *The Air Force Law Review*, no. 64 (2009): 147.

26. Matus, *Strategic Impact of Cyber Warfare Rules*, 31.

27. Wingfield, *Law of Information Conflict*, 290; International Committee of the Red Cross, "Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977" http://www.icrc.org/ihl.nsf/7c4d08d9b287a42141256739003e636b/f6c8b9fee14a77fdc125641e0052b079 (accessed December 7, 2010). Under this protocol, "works or installations containing dangerous forces, namely dams, dikes and nuclear electrical generating stations, shall not be made the object of attack, even where these objects are military objectives, if such attack may cause the release of dangerous forces and consequent severe losses among the civilian population."

28. Matus, *Strategic Impact of Cyber Warfare Rules*, 10; Wingfield, *Law of Information Conflict*, 352-354.

29. Todd, "Armed Attack in Cyberspace," 94. According to Todd, "while a criminal offense in virtually every nation state, espionage is not a violation of the law of war and was first recognized in the Lieber Code in 1863."

30. Attribution for cyberspace intrusions is historically very difficult. You can often attribute the attacks to certain computers based on their internet protocol (IP) addresses but these computers are often infected by robot networks directing the intrusions from other remote computers. This makes clear attribution to a responsible individual difficult. If you get that far, then proving the individual was operating in an official capacity as a representative of a foreign nation is an additional level of difficulty. The problems in attribution make deterrence by punishment challenging although deterrence through denial remains possible. For more information on the difficulty with attribution see Ashley, *Anatomy of Cyber Terrorism*, 25-26; and Beidleman, *Defining and Deterring Cyber War*, 3. For a detailed discussion of the difficulty with attribution and its effect on deterrence, see Libicki, *Cyberdetterence and Cyberwar*.

31. Wingfield, *Law of Information Conflict*, 8. According to Wingfield, "[even though] a non-state actor can cause identical damage to a state's information infrastructure as can a state actor, a hostile, transnational activity in cyberspace committed by a non-state actor remains a law enforcement issue. The issue of state and non-state sponsorship, however, may be very factually complicated by a number of circumstances such as the activities of state-owned commercial enterprises and

surrogate-actors, as well as the anonymity afforded by technology. Nevertheless, the legal analysis remains rather straightforward. Determining when state-owned commercial enterprises, for example, are acting as a commercial enterprise or at the direction of a state is a determination surrounding facts such as who controls the enterprise, who directed the activity, and the nature of the activity. It is not an issue of law. Consequently, from a legal perspective, all hostile transnational activities in cyberspace are either non-state-sponsored and thus a crime addressed by national and peacetime treaty law, or they are state-sponsored and thus a use of force governed by the law of conflict management and the law of armed conflict. The complete refusal or unwillingness of a state, however, to cooperate in the suppression or prevention of an acknowledged non-state-sponsored hostile, transnational activity in cyberspace that originates in its sovereign territory constitutes state-sponsorship of a use of force ipso facto, thereby invoking the law of conflict management which may authorize a use of force in self-defense against such a state or the non-state actors in that state. In the absence of any state-sponsorship of terrorist or criminal activities, a use of force by a state against those non-state actors in the sovereign territory of another state without that state's consent may rise to the level to be an unlawful use of force against that territorial state."

32. Stuart Biegel, *Beyond Our Control? Confronting the Limits of Our Legal System in the Age of Cyberspace* (Cambridge, MA: The MIT Press, 2001), 236; Michael L. Rustad, *Internet Law in a Nutshell* (St. Paul, MN: Thomson Reuters, 2009), 247; Robert W. Taylor et al., *Digital Crime and Digital Terrorism* (Upper Saddle River, NJ: Pearson Prentice Hall, 2006), 254-255.

33. Rustad, *Internet Law in a Nutshell*, 247-249.

34. Ibid., 246-247. For a more detailed discussion of botnets and how they are used, see Clay Wilson, "Cyber Crime," in *Cyberpower and National Security*, 420-422.

35. Ibid., 155-157.

36. Ibid., 53; Taylor, *Digital Crime and Digital Terrorism*, 255.

37. Ibid., 43 and 66.

38. Ibid., 58-60. France's prosecution of Yahoo! for hosting Nazi web sites is also noted in James A. Lewis, "Overcoming Obstacles to Cooperation: The Council of Europe Convention on Cybercrime," in *Cyber Security: Turning National Solutions into International Cooperation* (Washington, DC: The CSIS Press, 2003), 96.

39. Beidleman, *Defining and Deterring Cyber War*, 3.

40. Beidleman, *Defining and Deterring Cyber War*, 3; Kristin Archick, *Cybercrime: The Council of Europe Convention* (Washington, DC: Library of Congress, Congressional Research Service, September 28, 2006), 1; Michael Vatis, "International Cyber-Security Cooperation: Informal Bilateral Models," in *Cyber Security: Turning National Solutions into International Cooperation*, ed. James A. Lewis (Washington, DC: The CSIS Press, 2003), 7.

41. Clay Wilson, *Computer Attack and Cyberterrorism: Vulnerabilities and Policy Issues for Congress* (Washington, DC: Library of Congress, Congressional Research Service, April 1, 2005), 33; Archick, *Cybercrime*, 1; Rustad, *Internet Law in a Nutshell*, 256-257.

42. Archick, *Cybercrime*, 1; Henrik Kaspersen, "A Gate Must Either Be Open or Be Shut: The Council of Europe Cybercrime Convention Model," in *Cyber Security: Turning National Solutions into International Cooperation*, ed. James A. Lewis (Washington, DC: The CSIS Press, 2003), 16-18. Kaspersen describes the Convention's aims a little differently than Archick by stating five aims: harmonization of criminal law; harmonization of criminal procedural law concerning criminal investigations in public and private computer systems and networks; facilitate mutual legal assistance; codify international public law; and provide for an international legal framework.

43. Pottengal Mukundan, "Laying the Foundations for a Cyber-Secure World," in *Cyber Security: Turning National Solutions into International Cooperation*, ed. James A. Lewis (Washington, DC: The CSIS Press, 2003), 34.

44. Rustad, *Internet Law in a Nutshell*, 45.

45. Rebecca Grant, *Victory in Cyberspace* (Arlington, VA: Air Force Association, 2007), 8.

46. Baldor, "General Suggests 'Secure Zone.'"

47. Clarke and Knake, *Cyber War*, 267.

48. Bush, *National Strategy to Secure Cyberspace*, 2; U.S. Government Accountability Office, *Cybersecurity: Continued Efforts Are Needed to Protect Information Systems from Evolving Threats*, statement for the record to the Subcommittee on Terrorism and Homeland Security, Committee on the Judiciary, U.S. Senate (Washington, DC: U.S. Government Accountability Office, November 17, 2009), 12.

49. U.S. Government Accountability Office, *Cybersecurity: Progress Made but Challenges Remain in Defining and Coordinating the Comprehensive National Initiative*, report to Congressional requesters (Washington, DC: U.S. Government Accountability Office, March 2010), 17.

50. This categorization into six basic sources of threats was developed by the Federal Bureau of Investigation and cited in GAO, *Cybersecurity: Continued Efforts Needed*, 4.

51. Beidleman, *Defining and Detering Cyber War*, 18; Clarke and Knake, *Cyber War*, 144; U.S. General Accounting Office, "Information Security: Computer Attacks at Department of Defense Pose Increasing Risks," http://www.fas.org/irp/gao/aim96084.htm (accessed December 7, 2010). Clarke and Knake provide a more conservative estimate of over twenty nations with some cyber war capability.

52. GAO, *Cybersecurity: Continued Efforts Needed*, 4.

53. U.S. Congress, Senate, Select Committee on Intelligence, 15th Annual World-Wide Threat Hearing, *Current and Projected National Security Threats to the United States*, 111th Cong., 1st sess., February 12, 2009, 8; Clarke and Knake, Cyber War, 144. Clarke and Knake estimate that the United States has the most sophisticated cyber war capability followed closely by Russia, China and France.

54. Steven P. Bucci, *The Confluence of Cyber Crime and Terrorism* (Washington, DC: Heritage Foundation, June 12, 2009), 3; Daniel J. Busby, *Peacetime Use of Computer Network Attack*, Strategy Research Project (Carlisle Barracks, PA: U.S. Army War College, 2000), 1.

55. Wingfield, *Law of Information Conflict*, 24.

56. Cyber Security Strategy Committee, *Cyber Security Strategy* (Tallinn, Estonia: Ministry of Defence, 2008), 6.

57. Grant, *Victory in Cyberspace*, 4-9; Clarke and Knake, *Cyber War*, 15-16; Taylor, *Digital Crime and Digital Terrorism*, 27-28. Grant provides a detailed explanation of the CNA on Estonia and its implications for the future. Taylor provides further background on the forms of distributed denial of service attacks.

58. Korns and Kastenberg, "Georgia's Cyber Left Hook," 60; Clarke and Knake, *Cyber War*, 17-18.

59. Mark Clayton, "Stuxnet Malware is 'Weapon' Out to Destroy…Iran's Bushehr Nuclear Plant?," *Christian Science Monitor*, September 21, 2010; John Markoff and David E. Sanger, "In a Computer Worm, a Possible Biblical Clue," *New York Times*, September 29, 2010. This particular SCADA software was produced by Siemens, a German-based company, and is widely used in international industry.

60. Clayton, "Stuxnet Malware;" Thomas Erdbrink and Ellen Nakashima, "Iran Struggling to Contain 'Foreign-Made' Computer Worm, *Washington Post*, September 28, 2010; Associated Press, "Iran Accuses West of Computer Sabotage," *USA Today*, October 6, 2010.

61. Beidleman, *Defining and Deterring Cyber War*, 5; Libicki, *Cyberdeterrence and Cyberwar*, 2; Bruce Caulkins, *Proactive Self-Defense in Cyberspace* (Arlington, VA: The Institute of Land Warfare, 2009), 8.

62. Libicki, *Cyberdeterrence and Cyberwar*, 89.

63. GAO, *Cybersecurity: Continued Efforts Needed*, 4; Bucci, *Confluence of Cyber Crime*, 5; Caulkins, *Proactive Self-Defense*, 7.

64. William D. O'Neil, "Cyberspace and Infrastructure," in *Cyberpower and National Security*, 127; Wilson, "Cyber Crime," 433. According to O'Neil, the CIA has warned of this potential for cyber extortion noting that "cyber attackers have hacked into the computer systems of utility companies outside the United States and made demands, in at least one case causing a power outage that affected multiple cities." According to Wilson, in January 2008, the CIA stated

that "we have information, from multiple regions outside the United States, of cyber intrusions into utilities, followed by extortion demands."

65. Caulkins, *Proactive Self-Defense*, 8; Wilson, *Computer Attack and Cyberterrorism*, 20; Rustad, *Internet Law in a Nutshell*, 246. According to Rustad, "the U.S. Justice Department indicted a Brazilian cybercriminal, Leni de Abreu Neto, for participating in a conspiracy with a 19-year old man from the Netherlands, Nordin Nasiri, to use, maintain, lease and sell an illegal botnet."

66. GAO, *Cybersecurity: Continued Efforts Needed*, 4.

67. Ibid.

68. Ashley, *Anatomy of Cyber Terrorism*, 26-28; Beidleman, *Defining and Deterring Cyber War*, 3; James Glave, "Analyzer Nabbed in Israel?," *Wired News*, March 16, 1998; Jaxon Van Derbeken, Jim Doyle, and Glen Martin, "Hacking Suspect Caught in Cloverdale," *San Francisco Chronicle*, February 27, 1998.

69. Kevin Poulsen, "Slammer Worm Crashed Ohio Nuke Plant Network," *Security Focus*, August 19, 2003, http://www.securityfocus.com/news/6767 (accessed December 7, 2010).

70. Beidleman, *Defining and Deterring Cyber War*, 6; O'Neil, "Cyberspace and Infrastructure," 125; Wilson, *Computer Attack and Cyberterrorism*, 10-11; Robert Lemos, "MSBlast and the Northeast Power Outage," *CNet News*, February 16, 2005, http://news.cnet.com/8301-10784_3-5579309-7.html (accessed December 7, 2010); Dan Verton, "Blaster Worm Linked to Severity of Blackout," *Computerworld*, August 29, 2003, http://www.computerworld.com/printthis/2003/0,4814,84510,00.html (accessed December 7, 2010). There is some dispute over how significant the MSBlast or Blaster worm was in causing the blackout. According to Wilson, congestion caused by the Blaster worm delayed the exchange of critical power grid control data across the public telecommunications network, which could have hampered the operators' ability to prevent the cascading effect of the blackout. According to O'Neil, "investigation showed that neither al Qaeda nor Blaster was responsible."

71. GAO, *Cybersecurity: Continued Efforts Needed*, 4; Taylor, *Digital Crime and Digital Terrorism*, 92.

72. Libicki, *Cyberdeterrence and Cyberwar*, 62-63.

73. GAO, *Cybersecurity: Continued Efforts Needed*, 4; Taylor, *Digital Crime and Digital Terrorism*, 7. Some experts reason that insiders pose the greatest threat because of their access and knowledge of where to look for information in the network. Studies cited in Taylor's book attribute 73% to 90% of economic computer crimes to insiders.

74. Taylor, *Digital Crime and Digital Terrorism*, 60.

75. Clay Wilson, *Computer Attack and Cyberterrorism*, 6. United States law (Title 22 USC, section 2656) has employed this definition of terrorism for statistical and analytical purposes since 1983. The DoD definition, from U.S. Joint Chiefs

of Staff, Joint Publication 1-02, 468, is similarly worded: "the calculated use of unlawful violence or threat of unlawful violence to inculcate fear; intended to coerce or to intimidate governments or societies in the pursuit of goals that are generally political, religious, or ideological."

76. Wilson, *Computer Attack and Cyberterrorism*, 7. There is considerable debate over what constitutes cyber-terrorism. In Irving Lachow, "Cyber Terrorism: Menace or Myth?," in *Cyberpower and National Security*, 438, Lachow offers a more detailed definition of cyberterrorism as "a computer based attack or threat of attack intended to intimidate or coerce governments or societies in pursuit of goals that are political, religious, or ideological. The attack should be sufficiently destructive or disruptive to generate fear comparable to that from physical acts of terrorism. Attacks that lead to death or bodily injury, extended power outages, plane crashes, water contamination, or major economic losses would be examples." An important distinction is that terrorism is defined by the nature of the act not by the identity of the perpetrators. Use of the internet by terrorists for propaganda and recruiting should not be considered cyber-terrorism. Cyber-terrorism, consisting of an act of CNE or CNA by a terrorist group, must intend to result in the same effects as physical acts of terrorism such as violence against human targets or as Barry Collin of the Institute for Security and Intelligence puts it "hacking with a body count." For more on this debate and distinction see Taylor, *Digital Crime and Digital Terrorism*, 21-23.

77. Bucci, *Confluence of Cyber Crime*, 4; Clarke and Knake, *Cyber War*, 135.

78. John Arquilla and David Ronfeldt, "The Advent of Netwar (Revisited)," in *Networks and Netwars: The Future of Terror, Crime and Militancy* (Santa Monica, CA: RAND Corporation, 2001), 1-28; Clarke and Knake, *Cyber War*, 135.

79. Wilson, *Computer Attack and Cyberterrorism*, 6.

80. Baldor, "General Suggests 'Secure Zone.'"

81. Wilson, *Computer Attack and Cyberterrorism*, 19.

82. Ashley, *Anatomy of Cyberterrorism*, 29; Beidleman, *Defining and Deterring Cyber War*, 6; Permanent Monitoring Panel of Information Security, *Toward a Universal Order of Cyberspace: Managing Threats from Cybercrime to Cyberwar* (New York, NY: World Federation of Scientists, August 2003), 9; Kevin Poulsen, "FBI Issues Water Supply Cyberterror Warning," *Security Focus*, January 30, 2002, http://www.securityfocus.com/news/319 (accessed December 7, 2010); William Matthews, "Al Qaeda Cyber Alarm Sounded," Computer Crime Research Center, July 25, 2002, http://www.crime-research.org/news/2002/07/Mess2601.htm (accessed December 7, 2010); Taylor, *Digital Crime and Digital Terrorism*, 31.

83. Bucci, *Confluence of Cyber Crime*, 5-6; Taylor, *Digital Crime and Digital Terrorism*, 31. Taylor cites a statement from an Islamic cleric associated with bin Laden who indicates "fundamentalist Islamic groups are assembling cadres of computer science students sympathetic to al Qaeda's cause."

84. Ashley, *Anatomy of Cyber Terrorism*, 23; Taylor, *Digital Crime and Digital Terrorism*, 30-31. Taylor describes the combination of a CNA attack with a physical attack as an "adjunct attack" and discusses how it can be a force multiplier for the terrorist by enhancing the impact of the physical attack. For example, hacking into and disabling emergency response systems during a physical attack would hamper the response of rescue personnel.

85. Rustad, *Internet Law in a Nutshell*, 258-268; Taylor, *Digital Crime and Digital Terrorism*, 237-239 and 249-255. Both of these sources provide more detailed discussions of these federal statutes and their implications and constraints for intelligence and law enforcement officials.

86. Wingfield, *Law of Information Conflict*, 146 and 159.

87. Blair, *National Intelligence Strategy*, 5 and 9. Specifically the NIS stated mission objective is "Enhance cybersecurity – understand, detect, and counter adversary cyber threats to enable protection of the Nation's information infrastructure."

88. Ibid., 9.

89. Some experts believe it would require 2-4 years of surveillance, testing, and preparation and maybe even 6-10 years for a truly comprehensive mass disruption of multiple infrastructure networks. See Wilson, *Computer Attack and Cyberterrorism*, 17.

90. Blair, *National Intelligence Strategy*, 9.

91. U.S. Department of Homeland Security, *Cyber Storm Exercise Report*, 6-8. According to this report, the sheer volume of information constrained the ability of organizations to do both situational awareness and the second order technical analysis of networks and individuals.

92. James Jay Carafano, *The Future of Anti-Terrorism Technologies* (Washington, DC: Heritage Foundation, January 17, 2005), 5.

93. Rustad, *Internet Law in a Nutshell*, 30-31.

94. Kim Cragin et al., *Sharing the Dragon's Teeth: Terrorist Groups and the Exchange of New Technologies* (Santa Monica, CA: RAND Corporation, 2007), xvi and 97.

95. Ibid., xv and 94.

96. Wilson, *Computer Attack and Cyberterrorism*, 26.

97. Blair, *National Intelligence Strategy*, 9.

98. Ibid., 5.

99. GAO, *Cybersecurity: Progress Made*, 18.

100. Shaun Waterman, "Cyber Storm III Aims to Protect Against Real Thing," *Washington Times*, September 28, 2010.

101. U.S. Department of Homeland Security, *Cyber Storm Exercise Report*, 10.

Section Two:
Information Effects in the Cognitive Dimension

Can't Count It, Can't Change It: Assessing Influence Operations Effectiveness

1. Steve Booth-Butterfield, *Healthy Influence—Persuasion Blog: Communication for a Change*, http://healthyinfluence.com/wordpress/steves-primer-of-practical-persuasion-3-0/outro/the-rules/ (accessed November 3, 2010).
2. *Afghanistan: Where Things Stand*, (ABC News/BBC/ARD/Washington Post Poll, December 6, 2010), linked from Langer Research Associates Home Page, http://www.langerresearch.com/uploads/1116a1Afghanistan.pdf (accessed February 14, 2010).
3. Peter L. Burnett, *Information Operations,* Strategy Research Project (Carlisle Barracks, PA: U.S. Army War College, April 9, 2002), 7.
4. *The Free Dictionary*, http://www.thefreedictionary.com/influence (accessed November 3, 2010).
5. U.S. Department of the Air Force, *Information Operations*, Air Force Doctrine Document 2-5 (Washington, DC: U.S. Department of the Air Force, January 11, 2005), 9.
6. Ibid.
7. U.S. Joint Chiefs of Staff, *Information Operations*, Joint Publication 3-13 (Washington DC: U.S. Joint Chiefs of Staff, February 13, 2006), I-1.
8. U.S. Joint Chiefs of Staff, *Joint Operations*, Joint Publication 3-0 (Washington DC: U.S. Joint Chiefs of Staff, September 17, 2006 Incorporating Change 2 March 22, 2010), III-36.
9. U.S. Joint Chiefs of Staff, *Joint Operation Planning*, Joint Publication 5-0 (Washington DC: U.S. Joint Chiefs of Staff, September 10, 2010), II-9, II-10.
10. Dennis M. Murphy, "In Search of the Art and Science of Strategic Communications," *Parameters* 39, no. 4 (Winter 2009-10): 107.
11. U.S. Army War College, *Information Operations Primer* (Carlisle Barracks, PA: U.S. Army War College, November, 2010), 2.
12. Walt Kelly, *Pogo: We Have Met the Enemy and He Is Us* (New York: Simon and Schuster, 1972, 1987). The quote is drawn from the title of this publication.
13. *PSYOP Regimental Blog*, http://psyopregiment.blogspot.com/2010/06/miso-is-it-soup-yet.html (accessed November 6, 2010).
14. Murphy, "In Search of the Art and Science of Strategic Communications," 109.
15. Ibid., 110.

16. David H. Sammons, *PSYOP and the Problem of MOE for the Combatant Commander*, Strategic Research Paper (Newport, RI: U.S. Naval War College, April 18, 2004), 1.
17. J. Michael Waller, "Murtha axes military information operations for FY2010," *Politicalwarfare.org Blog*, July 27, 2009, http://politicalwarfare.org/ (accessed November 7, 2009).
18. Peter Cary, *The Pentagon, Information Operations, and International Media Development* (Washington DC: Center for International Media Assistance, October 19, 2010), 5.
19. Ibid.
20. Ibid., 37.
21. Barack Obama, *National Framework for Strategic Communication* (Washington DC: The White House, March 16, 2010), 13.
22. Julia Coffman, *Public Communication Campaign Evaluation: An Environmental Scan of Challenges, Criticisms, Practice, and Opportunities* (Washington DC: Communications Consortium Media Center, May 2002), 13.
23. U.S. Joint Chiefs of Staff, *Joint Operations*, GL-20.
24. Ibid.
25. Coffman, *Public Communication Campaign Evaluation: An Environmental Scan of Challenges, Criticisms, Practice, and Opportunities*, 13.
26. Ibid.
27. Ibid., 15.
28. Ibid., IV-27.
29. Basil Liddell Hart, "Thoughts on Philosophy, Politics & Military Matters," (Liddell Hart Papers II, June 7, 1932), 20.
30. Gregory S. Seese, "Measuring Psychological Operations: It's All About the SPO," *Special Warfare* 22, issue 5 (September-October 2009): 10-11.
31. Icek Ajzen, "The Social Psychology of Decision Making," in *Social Psychology: Handbook of Basic Principles*, ed. E. T. Higgins and A. W. Kruglanski (New York: Guilford Press, 1996), 297.
32. Mark Melvin, "Program Evaluation," in *Handbook of Psychology, Volume 2, Research Methods in Psychology*, ed. John A. Schinka, Wayne F. Velicer, and Irving B. Weiner (Hoboken, NJ: John Wiley & Sons, Inc., 2003), 324.
33. U.S. Joint Forces Command, *Commander's Handbook for Strategic Communications and Communication Strategy* (Suffolk, VA: U.S. Joint Forces Command, June 24, 2010): IV-27.
34. Donald Neff, "Quantitative Research Designs for MOE," *Mind Games* 2, no. 3 (Joint Military Information Support Command, March 31, 2010): 1.

35. Icek Ajzen, Theory of Planned Behavior Diagram (2006) http://people.umass.edu/aizen/tpb.diag.html (accessed 12 October 2010).
36. Icek Ajzen, "The Theory of Planned Behavior," *Organizational Behavior and Human Decision Processes* 50 (1991), 179-211.
37. Anthony R. Pratkanis, email message to author, December 9, 2010. Dr. Pratkanis is a Professor of Psychology at the University of California in Santa Cruz, California. Dr. Pratkanis is an expert on economic fraud crimes, terrorist and dictator propaganda, marketing and consumer behavior, and persuasion and influence.
38. Murphy, "In Search of the Art and Science of Strategic Communications," 111.
39. U.S. Department of the Army, *Psychological Operations Tactics, Techniques, and Procedures*, Field Manual 3-5.301 (Washington DC: U.S. Department of the Army, August 2007), viii.
40. Murphy, "In Search of the Art and Science of Strategic Communications," 106.
41. U.S. Joint Forces Command, *Commander's Handbook for Strategic Communications and Communication Strategy*, O-9.
42. Ibid., O-11.
43. Christopher Rate, *JMISC Assessment Program* (Tampa, FL: Joint Military Information Support Command, November 17, 2009), 1.
44. Ibid.
45. Murphy, "In Search of the Art and Science of Strategic Communications," 109.
46. Cary, *The Pentagon, Information Operations, and International Media Development*, 9.
47. Ibid., 11.
48. Ibid., 11-12.
49. U.S. Joint Chiefs of Staff, *Joint Operation Planning*, III-5.
50. Murphy, "In Search of the Art and Science of Strategic Communications," 113-114.
51. Ibid., 111.
52. U.S. Department of the Air Force, *Military Information Support Operations*, Air Force Instruction 10-702 (Washington DC: U.S. Department of the Air Force, Draft), 6.
53. Murphy, "In Search of the Art and Science of Strategic Communications," 115.

Strategic Communiation: The Meaning is in the People

1. Scott M. Cutlip, Allen H. Center, Glen M. Broom, eds., *Effective Public Relations* (Upper Saddle River, New Jersey: Prentice-Hall, Inc., 2000), 249.

2. Joseph S. Nye, "The New Public Diplomacy," February 10, 2010, linked from Project Syndicate at http://www.project-syndicate.org (accessed October 19, 2010).
3. Michael G. Mullen, "Strategic Communication: Getting Back to Basics," *Joint Force Quarterly* 55, (4th Quarter 2009), 2.
4. U.S. Department of Defense, *Capstone Concept for Joint Operations Version 3.0*, (Washington, DC; Department of Defense, January 15, 2009), 5; Andrew Mackay and Steve Tatham, "Behavioural Conflict from General to Strategic Corporal: Complexity, Adaptation and Influence," *The Shrivenham Papers*, no 9 (December 2009): 13.
5. Carl Von Clausewitz, *On War*, eds. & trans. Michael Howard and Peter Paret (Princeton: Princeton University Press, 1976), 119.
6. Mullen, "Strategic Communication: Getting Back to Basics," 2.
7. J. Michael Waller, Ph.D., "Strategic Global Influence for the United States," *Congressional Record* (March 4, 2010).
8. Steven Metz, "Why General Petraeus is Better Suited for Our Afghanistan Mission than General McChrystal Ever Was," June 24, 2010, linked from *The New Republic* at http://www.tnr.com (accessed November 2, 2010).
9. The author asked the question to the visiting general officer that rendered this response. Non attribution ground rules were in affect during this discussion.
10. U.S. Department of Defense Office, *Final Report of the Defense Science Board Task Force on Strategic Communication* (Washington, DC: U.S. Defense Science Board, January 4, 2008), 14.
11. Cutlip, Center, and Broom, *Effective Public Relations*, 252.
12. Wilbur Schramm and Donald E. Roberts, eds., *The Process and Effects of Mass Communication* (Urbana, IL: University of Illinois Press, 1972): 7.
13. David K. Berlo, *The Process of Communication: An Introduction to Theory and Practice* (New York, NY: Holt, Rinehart and Winston, Inc., 1960): 11-12.
14. Cutlip, Center, and Broom, *Effective Public Relations*, 253.
15. Schramm and Roberts, *The Process and Effects of Mass Communications*, 17.
16. U.S. Department of Defense Office, *Final Report of the Defense Science Board Task Force on Strategic Communication*, 11.
17. Steven R. Corman, Angela Trethewey, H.L. Goodall, Jr., eds., *Weapons of Mass Persuasion: Strategic Communication to Combat Violent Extremism* (New York, NY: Peter Land Publishing, Inc., 2008): 6.
18. Ibid., 156.
19. Berlo, *The Process of Communication: An Introduction to Theory and Practice*, 175.

20. Corman, Trethewey, and Goodall, *Weapons of Mass Persuasion: Strategic Communication to Combat Violent Extremism*, 5.
21. *Democratic Rep Steve Cohen Defends Comparison of GOP Health Law Attacks to Nazi 'Lies*,' http://www.foxnews.com/politics (accessed January 30, 2011).
22. Corman, Trethewey, and Goodall, *Weapons of Mass Persuasion: Strategic Communication to Combat Violent Extremism*, 157.
23. Barack Obama, *Remarks by President on the Situation in Egypt*, February 1, 2011, www.whitehouse.gov, (accessed February 3, 2011).
24. Corman, Trethewey, and Goodall, *Weapons of Mass Persuasion: Strategic Communication to Combat Violent Extremism*, 156.
25. Nye, "The New Public Diplomacy."
26. Mullen, "Strategic Communication: Getting Back to Basics," 3.
27. Kenneth Payne, "Waging Communication War," *Parameters* 38, no. 2 (Summer 2008): 38.
28. Mullen, "Strategic Communication: Getting Back to Basic," 4.
29. Principal Deputy Assistant Secretary of Defense for Public Affairs Robert T. Hastings, "Principles of Strategic Communication Guide," memorandum for Secretaries of the Military Departments, Washington, DC, August 15, 2008.
30. Berlo, *The Process of Communication: An Introduction to Theory and Practice*, 30-31.
31. Corman, Trethewey, and Goodall, *Weapons of Mass Persuasion: Strategic Communication to Combat Violent Extremism*, 5.
32. Aaron Hess and Z.S. Justus, "Re-Defining the Long War: Toward a New Vocabulary of International Terrorism," in *Weapons of Mass Persuasion: Strategic Communication to Combat Violent Extremism*, eds., Steven Corman, Angela Trethewey, and H.L. Goodall, Jr., (New York, NY: Peter Land Publishing, Inc., 2008): 129, 131.
33. Ibid., 133.
34. Corman, Trethewey, and Goodall, *Weapons of Mass Persuasion: Strategic Communication to Combat Violent Extremism*, 6.
35. *Sensemaking*, http://en.wikipedia.org/wiki/Sensemaking#cite_note-Weick1995-2 (accessed November 13, 2010).
36. Ibid.
37. Corman, Trethewey, and Goodall, *Weapons of Mass Persuasion: Strategic Communication to Combat Violent Extremism*, 151, 4-5.
38. The author served as a Public Affairs Officer in USEUCOM from August 2008 to June 2010 and during this time he was a member of the Strategic

Communication Working Group and Strategic Communication Executive Board.

39. Corman, Trethewey, and Goodall, *Weapons of Mass Persuasion: Strategic Communication to Combat Violent Extremism*, 30.
40. Cutlip, Allen, and Broom, *Effective Public Relations*, 251.
41. Schramm and Roberts, *The Process and Effects of Mass Communications*, 8.
42. Ibid.
43. Corman, Trethewey, and Goodall, *Weapons of Mass Persuasion: Strategic Communication to Combat Violent Extremism*, 157, 30.
44. Ibid., 159.
45. Ibid., 11-12, 157.
46. Ibid.
47. U.S. Department of Defense Office, *Final Report of the Defense Science Board Task Force on Strategic Communication*, 14.
48. Corman, Trethewey, and Goodall, *Weapons of Mass Persuasion: Strategic Communication to Combat Violent Extremism*, 166.
49. Ibid.
50. U.S. Army General David H. Petraeus, "COMISAF's Counterinsurgency Guidance," memorandum for Soldiers, Sailors, Airmen, Marines and Civilians of NATO ISAF and U.S. Forces-Afghanistan, Kabul, Afghanistan, August 1, 2010.
51. Ibid.
52. Payne, "Waging Communication War," 37.
53. Helmus, Paul, Glen, *Enlisting Madison avenue: The Marketing Approach to Earning Popular Support in Theaters of Operation* (Santa Monica: RAND Corporation, 2007), 26.
54. Ibid., xiii.
55. Ibid., 10.
56. Ibid., xiii, 45.
57. Corman, Trethewey, and Goodall, *Weapons of Mass Persuasion: Strategic Communication to Combat Violent Extremism*, 159.
58. Cutlip, Allen, and Broom, *Effective Public Relations*, 450.
59. Ibid.
60. Corman, Trethewey, and Goodall, *Weapons of Mass Persuasion: Strategic Communication to Combat Violent Extremism*, 43.
61. Ibid., 159.

62. Cutlip, Allen, and Broom, *Effective Public Relations*, 254.
63. Helmus, Paul, and Glen, *Enlisting Madison Avenue: The Marketing Approach to Earning Popular Support in Theaters of Operation*, 32.
64. Cutlip, Allen, and Broom, *Effective Public Relations*, 258, 259.
65. Corman, Trethewey, and Goodall, *Weapons of Mass Persuasion: Strategic Communication to Combat Violent Extremism*, 159.
66. Schramm and Roberts, *The Process and Effects of Mass Communications*, 38.
67. Cutlip, Allen, and Broom, *Effective Public Relations*, 449.
68. Bruce Hoffman, *Influence Warfare: How Terrorists and Governments Fight to Shape Perception in a War of Ideas*, ed. James J.F. Forest (Westport: Praeger Security International, 2009): viii.
69. Cutlip, Allen, and Broom, *Effective Public Relations*, 425.

Section Three: Information Sharing

Introduction

1. John M. McConnell, *Intelligence Community Information Sharing Strategy* (Washington, DC: U.S. Intelligence Community, February 22, 2008), 8.

DOD Information Sharing with Domestic Emergency Partners for Defense Support of Civil Authorities Missions

1. Charles Rodriguez, Bernd McConnell and Kristine Shelstad, "Support to Disaster Response: The Science and Art of Disaster Response by the National Guard," *Center for Army Lessons Learned Newsletter*, 10-16 (Fort Leavenworth, KS: U.S. Department of the Army, December 2009), 39, http://usacac.army.mil/CAC2/call/docs/10-16/ch_7.asp (accessed January 2, 2012).
2. U.S. Department of the Army, *Civil Support Operations*, FM 3-28 (Washington, DC: U.S. Department of the Army, August 20, 2010), 1-15, http://usacac.army.mil/cac2/FM3-28/FM328.pdf (accessed January 2, 2012).
3. George W. Bush, "Homeland Security Presidential Directive 5: Management of Domestic Incidents," February 28, 2003, http://www.dhs.gov/xabout/laws/gc_1214592333605.shtm (accessed January 2, 2012).
4. U.S. Department of Homeland Security, "Introducing National Response Framework," January 2008, 3, http://www.fema.gov/pdf/emergency/nrf/about_nrf.pdf (accessed January 2, 2012).
5. Tribal government entities are commonly listed in emergency management documents including the National Response Framework. FEMA refers to the Title 25 (Indians) and Title 43, Chapter 33 (Alaska Native Claims Settlement)

in defining Indian Tribes and Tribal Governments. Federal Emergency Management Association, "Disaster Assistance Policy 9521.4: Administering American Indian and Alaska Native Tribal Government Funding," (April 30, 2007), http://www.fema.gov/government/grant/pa/9521_4.shtm (accessed January 2, 2012).

6. U.S. Department of Homeland Security, "Introducing National Response Framework," 3.

7. The term mutual aid/assistance agreement as used here includes cooperative agreements, partnership agreements, memoranda of understanding, intergovernmental compacts, or other terms commonly used for the sharing of resources. National Fire Protection Association, "NFPA 1600: Standard on Disaster/Emergency Management and Business Continuity Programs," 2007 ed., *National Fire Codes Subscription Service*, Electronic Edition, CD-ROM, (Quincy, MA: NFPA International, Fall 2008), Appendix A.

8. Title 32 of the U.S. Code outlines the dual status role of members of the National Guard, serving under the Governor of each state or territory until ordered to active duty (Title 10) status, serving under the command of the President of the United States. The Governor has the ability to mobilize Soldiers and Airmen to state active duty status according to the laws of their State. In this status, the provisions of the Posse Comitatus Act do not apply. U.S. Army National Guard, "National Guard Fact Sheet Army National Guard (FY2005)," May 3, 2006, http://www.arng.army.mil/SiteCollectionDocuments/Publications/News%20Media%20Factsheets/ARNG_Factsheet_May_06%20ARNG%20fact%20Sheet.pdf (accessed January 2, 2012).

9. The Federal share for assistance provided under this title (section) shall not be less than 75 percent of the eligible costs (of such assistance). *Cost Sharing*, U.S. Code of Federal Regulations, 44, sec. 206.65 (1990), http://ecfr.gpoaccess.gov/cgi/t/text/text-idx?c=ecfr&sid=cb026ad7b49625e3d72368148b7e0bfb&rgn=div8&view=text&node=44:1.0.1.4.57.3.18.5&idno=44 (accessed January 2, 2012); Federal Emergency Management Agency, *Robert T. Stafford Disaster Relief and Emergency Assistance Act, as amended, and Related Authorities*, FEMA 592 (June 2007), 28, http://www.fema.gov/pdf/about/stafford_act.pdf (accessed January 2, 2012); also known as Public Law 93-288, as amended, U.S. Code, vol. 42, secs. 5121-5207.

10. Terry Scherling, "Examining the Military's Support of Civil Authorities during Disasters," (prepared statement to House of Representatives, Committee on Homeland Security, Subcommittee on Emergency Communications, Preparedness, and Response), 110th Cong., 1st sess. (April 25, 2007), (Washington, DC: U.S. Government Printing Office, 2009), 6, http://www.fas.org/irp/congress/2007_hr/disaster.pdf (accessed January 2, 2012).

11. Emergency Management Assistance Compact agreements are created between states to provide civilian and military assistance as permitted by Public Law 104-321. Procedures allow reimbursement for personnel and equipment and define

liability issues. *Emergency Management Assistance Compact, "What is EMAC?"* http://www.emacweb.org/index.php?option=com_content&view=article&id+80&Itemid=256 (accessed January 2, 2012).

12. Federal Emergency Management Agency, *Robert T. Stafford Disaster Relief and Emergency Assistance Act, as amended, and Related Authorities*, 28.

13. U.S. Department of Homeland Security, "National Response Framework," (Washington DC: U.S. Department of Homeland Security, January 2008), 6, http://www.fema.gov/pdf/emergency/nrf/nrf-core.pdf (accessed January 2, 2012).

14. Title 10 of the U.S. Code defines the role of the active duty military and the reserve component of the armed forces. The provisions of the Posse Comitatus Act typically apply to the duties of Title 10 Soldiers serving in the Continental United States as defined by 10 USC 375. Cornell University Law School, "Title 10 – Armed Forces," http://www.law.cornell.edu/uscode/uscode10/usc_sup_01_10.html (accessed January 2, 2012).

15. U.S. Joint Chiefs of Staff, *Department of Defense Dictionary of Military and Associated Terms*, Joint Publication 1-02, (Washington, DC: U.S. Joint Chiefs of Staff, November 8, 2010, as amended through January 31, 2011), 100, http://www.dtic.mil/doctrine/dod_dictionary (accessed January 2, 2012); U.S. Joint Chiefs of Staff, *Civil Support*, Joint Publication 3-28 (Washington, DC: U.S. Joint Chiefs of Staff, September 14, 2007), GL-7, http://www.dtic.mil/doctrine/new_pubs/jp3_28.pdf (accessed January 2, 2012).

16. According to Assistant Secretary of Defense for Homeland Defense Paul McHale. "McHale: Disaster Response Time Expected to Improve." *National Defense*, May 2006, http://www.thefreelibrary.com/McHale%3a+disaster+response+time+expected+to+improve.-a0145836347 (accessed January 2, 2012).

17. Sara Wood, "DOD Leaders Report on Hurricane Response," *American Forces Information Service News Articles*, November 10, 2005, http://osd.dtic.mil/news/Nov2005/20051110_3310.html (accessed January 2, 2012).

18. "Any occurrence, resulting from the use of chemical, biological, radiological and nuclear weapons and devices; the emergence of secondary hazards arising from counterforce targeting; or the release of toxic industrial materials into the environment, involving the emergence of chemical, biological, radiological and nuclear hazards." U.S. Joint Chiefs of Staff, *Department of Defense Dictionary of Military and Associated Terms*, Joint Publication 1-02, 51. A CBRN incident may be a manmade attack: such as an intentional sarin gas or radiological explosive (dirty bomb) attack, or intentionally spread biological event (anthrax or botulism contamination); manmade accident such as a chemical or nuclear plant incident; or natural occurrence, such as a pandemic influenza epidemic.

19. U.S. Joint Chiefs of Staff, *Department of Defense Dictionary of Military and Associated Terms*, Joint Publication 1-02, 114; U.S. Joint Chiefs of Staff, *Homeland Security*, Joint Publication 3-27 (Washington, DC: U.S. Joint Chiefs

of Staff, July 12, 2007), GL-8, http://www.dtic.mil/doctrine/new_pubs/jp3_27.pdf (accessed January 2, 2012).

20. Rodriguez, "Support to Disaster Response: The Science and Art of Disaster Response by the National Guard," 41.

21. GEN James Cartwright (speech presented to the general session of the National Guard Bureau's 2011 Domestic Operations Workshop, National Harbor, MD, January 20, 2011).

22. Ibid.

23. Frances Fragos Townsend, *The Federal Response to Hurricane Katrina: Lessons Learned* (Washington, DC: The White House, February 2006), 50, http://georgewbush-whitehouse.archives.gov/reports/katrina-lessons-learned/ (accessed January 2, 2012).

24. Controlled Unclassified Information (CUI) is defined by Executive Order 13556, dated November 4, 2010. U.S. National Archives and Records Administration, Office of the Federal Register, "Presidential Documents: Executive Order 13556," *Federal Register* 75, no. 216, (November 9, 2010), 68675, http://frwebgate.access.gpo.gov/cgi-bin/getpage.cgi?position=all&page=68675&dbname=2010_register (accessed January 2, 2012). Controlled unclassified information (CUI) is defined for the purposes of military compliance with this executive order by U.S. Department of the Army, *Operations Security*, Army Regulation 530-1, (Washington, DC: U.S. Department of the Army, April 19, 2007), 25, http://armypubs.army.mil/epubs/530_series_collection_1.html (accessed January 2, 2012).

25. Sensitive information is defined by the *Computer Security Act of 1987*, Public Law 100-135, 100th Cong., 1st sess. (January 8, 1988), http://www.nist.gov/cfo/legislation/Public%20Law%20100-235.pdf (accessed January 2, 2012).

26. Protected Critical Infrastructure Information is defined in *Homeland Security Act of 2002: Critical Infrastructure Information Act*, Public Law 107-296 (Title II, Subpart B), 107th Cong., 2nd sess. (November 25, 2003), http://www.dhs.gov/xlibrary/assets/CII_Act.pdf (accessed January 2, 2012).

27. Health insurance information security is defined in Department of Health and Human Services, Office of Civil Rights, "Summary of the Privacy Rule" (May 2003), http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/index.html (accessed January 2, 2012); *Health Insurance Portability and Accountability Act of 1996*, Public Law 104-191, 104th Cong., 2nd sess. (August 21, 1996), http://www.gpo.gov/fdsys/pkg/PLAW-104publ191/html/PLAW-104publ191.htm (accessed January 2, 2012).

28. *Freedom of Information Act (FOIA)*, U.S. Code, vol. 5, secs. 552, as amended by Public Law 104-231, Public Law 104-231, 104th Cong., 2nd sess. (October 2, 1996), http://www.justice.gov/oip/foia_updates/Vol_XVII_4/page2.htm (accessed January 2, 2012). For Official Use Only designations on documents produced by the U.S. Military are governed by U.S. Department of Defense, *The*

DOD Freedom of Information Act Program, Department of Defense Regulation 5400.7-R (Washington, DC: U.S. Department of Defense, September 4, 1998), http://www.dtic.mil/whs/directives/corres/pdf/540007r.pdf (accessed January 2, 2012).

29. These steps are also in keeping with the Federal Emergency Management Agency's National Emergency Communications Plan recommendations. *Communications and Information Management Page*, "Frequently Asked Questions," http://www.fema.gov/emergency/nims/CommunicationsInfoMngmnt.shtm#item3 (accessed January 2, 2012).

30. Commonly referred to as the '.mil' or 'dot mil' domain.

31. Gina Pace, "Mexico Sends First-Ever Aid North: 'Act of Solidarity' Brings Supplies, Specialists to the U.S.," *CBS News* (September 7, 2005), http://www.cbsnews.com/stories/2005/09/07/katrina/main824295.shtml (accessed January 2, 2012).

32. Christopher Evanson, "Canadian Beacon-Operation Unison," *Coast Guard Magazine* (Katrina The Gulf Response, Special Edition 2005), reprint, *Mariners Weather Log* (April 2006), http://www.vos.noaa.gov/MWL/apr_06/canada.shtml (accessed January 2, 2012).

33. Canada Command Joint Command Centre and NORAD and USNORTHCOM Command Center, "Strategic Operations Information Sharing Plan of Action," (December 18, 2009), https://www.intelink.gov/inteldocs/action.php?kt_path_info=ktcore.actions.document.view&fDocumentId=236155 (accessed January 2, 2012, Intelink account and password required).

34. *Walmart History Page*, http://walmartstores.com/AboutUs/297.aspx (accessed January 2, 2012).

35. Bryan Koon, "Emergency Management in the Private Sector," (speech presented to the general session of the 2010 New Madrid Seismic Zone Workshop, Camp Robinson, North Little Rock, AR, September 15, 2010).

36. Ibid.

37. Eli Noam and Harumasa Sato, "Kobe's lesson: dial 711 for 'open' emergency communications," *Science*, November 1, 1996, 739-740, http://www.citi.columbia.edu/elinoam/articles/kobe.htm (accessed January 2, 2012); quoted in Anthony Townsend and Mitchell Moss, "Telecommunications Infrastructure in Disasters: Preparing Cities for Crisis Communications" (April 2005), 38, http://www.nyu.edu/ccpr/pubs/NYU-DisasterCommunications1-Final.pdf (accessed January 2, 2012).

38. Belgrade, formerly capitol of Yugoslavia, is now the capitol of Serbia.

39. EL Quarantelli, "The Disaster Research Center (DRC) Field Studies of Organized Behavior in the Crisis Time Period of Disasters," Disaster Research Center, University of Deleware (1997); quoted in Townsend and Moss, "Telecommunications Infrastructure in Disasters: Preparing Cities for Crisis Communications," 34.

40. "From Disaster to Community Development: The Kobe Experience," United Nations Center for Regional Development (January 17, 2003), http://www1.reliefweb.int/rw/lib.nsf/db900SID/LHON-696JH2?OpenDocument; quoted in Townsend and Moss, "Telecommunications Infrastructure in Disasters: Preparing Cities for Crisis Communications," 34.

41. Ibid.

42. Anne Nelson, Ivan Sigal, and Dean Zambrano, *Media, Information Systems and Communities: Lessons from Haiti*, 12, http://issuu.com/knightfoundation/docs/kf_report_haiti_english_01.10.11?mode=embed&layout=http%3A%2F%2Fskin.issuu.com%2Fv%2Flight%2Flayout.xml&showFlipBtn=true (accessed January 2, 2012); *Christchurch Recovery Map Home Page*, http://eq.org.nz (accessed May 5, 2011).

43. Geotagging, also referred to as geo-referenced information or geospatial information "…is marking a video, photo or other media with a location." Daniel Nations, "What is Geotagging?" *About.com*, http://webtrends.about.com/od/glossary/a/what-geotagging.htm (accessed January 2, 2012).

44. During the Missouri River floods of the summer of 2011, the U.S. Army Corps of Engineers, Omaha District, regularly shared critical information such as reservoir inflow, outflow, and level status on Twitter and Facebook. *U.S. Army Corps of Engineers Omaha District Twitter Page*, https://twitter.com/#!/OmahaUSACE (accessed January 2, 2012); and *U.S. Army Corps of Engineers Omaha District Facebook Page*, http://www.facebook.com/OmahaUSACE (accessed January 2, 2012).

45. Microsoft® and SharePoint® are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

46. ESi® and WebEOC® are registered trademarks of ESi Acquisition, Inc. Product data sheet listing WebEOC clients listed at ESI Clients Page, http://esi911.com/esi/index.php?option=com_content&task=view&id=33&Itemid=44 (accessed January 2, 2012).

47. NC4™ and E Team are registered trademarks of NC4. Product data sheet available from *NC4 E Team Page*, http://www.nc4.us/eteam.php (accessed January 2, 2012).

48. Henry Kenyon, "National Guard Looks to Connect Nationwide," *Signal Online*, July 2008, http://www.afcea.org/signal/articles/templates/Signal_Article_Template.asp?articleid=1645&zoneid=237 (accessed January 2, 2012).

49. Federal Emergency Management Agency, *Communications and Information Management Page*, "Frequently Asked Questions."

50. ArcGIS® is a trademark or registered trademark of Environmental Systems Research Institute, Inc. (ESRI) in the United States, the European Community, or certain other jurisdictions.

51. Google Earth™ is a trademark or registered trademark of Google®.

52. Common file formats include KML, KMZ and GeoRSS. KML, known as Keyhole Markup Language when it was originally developed, is now an open standard officially named the OpenGIS® KML Encoding Standard (OGC KML) maintained by the Open Geospatial Consortium, Inc. (OGC). *Google Code KML Reference Page*, http://code.google.com/apis/kml/documentation/kmlreference.html (accessed January 2, 2012). KMZ files are compressed collections of KML files. Google Code KMZ Files, http://code.google.com/apis/kml/documentation/kmzarchives.html (accessed January 2, 2012). GeoRSS (Geographical information sent with RSS – Really Simple Syndication, a common web feed format) with GML, Geographical Markup Language, is another format for modeling, transport, and storage of geographic information, *Open Geospatial Consortium Geographical Markup Language*, http://www.opengeospatial.org/standards/gml (accessed January 2, 2012).

53. Nelson, Sigal, and Zambrano, *Media, Information Systems and Communities: Lessons from Haiti*, 5.

54. Ibid., 4.

55. Short codes are special telephone numbers, shorter than regular numbers, designed to facilitate easy SMS text services. Ibid., 12.

56. Ibid., 15.

57. Ibid., 13.

58 Ushahidi is "open source software for information collection, visualization and interactive mapping….using multiple channels, including SMS, email, Twitter and the web." *Ushahidi Home Page*, http://www.ushahidi.com (accessed January 2, 2012).

59. The bandwidth restrictions experienced by the Marines in this case could apply to any organization, military or otherwise, depending on the equipment they have available. This example highlights how it is helpful for data to be made available across different platforms. Nelson, Sigal, and Zambrano, *Media, Information Systems and Communities: Lessons from Haiti*, 13.

60. *Christchurch Recovery Map Home Page*.

61. Nelson, Sigal, and Zambrano, *Media, Information Systems and Communities: Lessons from Haiti*, 15; and *Christchurch Recovery Map Becoming a Volunteer*, http://eq.org.nz/page/index/9 (accessed May 5, 2011).

62. *Christchurch Recovery Map Becoming a Volunteer*.

63. Craig Fugate, "Understanding the Power of Social Media as a Communication Tool in the Aftermath of Disasters," (testimony before the Senate Committee on Homeland Security and Governmental Affairs, Subcommittee on Disaster Recovery and Intergovernmental Affairs, Washington, D.C., May 5, 2011), http://www.dhs.gov/ynews/testimony/testimony_1304533264361.shtm (accessed January 2, 2012).

64. "Crowdsourcing, a term coined by Jeff Howe in a June 2006 issue of *Wired* magazine, is a model of labor that has been fully embraced on the Internet…. [and] takes tasks traditionally done by a single person or small groups of people, and farms them out to a global workforce. The large-scale committee approach is powerful because it leans on the concept of the "wisdom of crowds" (to a certain extent) which says basically that the more input, the better the output." Jeff Howe, "The Rise of Crowdsourcing," *Wired* 14, June 2006, http://www.wired.com/wired/archive/14.06/crowds.html (accessed January 2, 2012); quoted in Josh Cantone, "Your Guide to the Crowdsourced Workforce," The *ReadWriteWeb*, May 12, 2008, http://www.readwriteweb.com/archives/crowdsourced_workforce_guide.php (accessed January 2, 2012); Kim Stephens, "Crisis Mapping, Crisis Crowdsourcing and Southern Storms," *idisaster 2.0: Social Media and Emergency Management*, May 8, 2011, http://idisaster.wordpress.com/2011/05/08/crisis-mapping-crisis-crowdsouring-and-southern-storms/ (accessed January 2, 2012).

65. Corey McKenna, "Social Network Adds Situational Awareness to Haitian Earthquake Response," *Emergency Management*, June 30, 2010, http://www.emergencymgmt.com/safety/Social-Network-Situational-Awareness-Haiti-Earthquake.html (accessed January 2, 2012).

66. "TweetGrid is a powerful Twitter Search Dashboard that allows you to search for up to 9 different topics, events, conversations, hashtags, phrases, people, groups, etc in real-time. As new tweets are created, they are automatically updated in the grid. No need to refresh the page!" *Tweetgrid FAQ*, http://tweetgrid.com/faq (accessed January 2, 2012). TweetDeck is another Twitter dashboard that is currently popular. *TweetDeck Home Page*, http://www.tweetdeck.com (accessed January 2, 2012).

67. Brenda Stoltz, "FEMA Administrator Wm. Craig Fugate on Social Media at GEOINT 2011," *Following the Thread*, http://www.ariadpartners.com/blog/bid/70001/FEMA-Administrator-Wm-Craig-Fugate-on-Social-Media-at-GEOINT-2011 (accessed January 2, 2012).

68. Ibid.

69. U.S. Department of Homeland Security, "National Incident Management System" (Washington, DC: U.S. Department of Homeland Security, December 2008), 70, http://www.fema.gov/pdf/emergency/nims/NIMS_core.pdf (accessed January 2, 2012).

70. COL Greg Hapgood, Iowa National Guard Public Affairs Officer (with Joint Information Center experience during domestic operations), interview by author, written notes, Johnston, IA, 02 May 2011.

71. Anne-Marie Corley, "Why Haiti's Cellphone Networks Failed: Haitian engineer Charles-Edouard Denis describes the cellular landscape before and after Haiti's quake," *IEEE Spectrum*, February 2010, http://spectrum.ieee.org/telecom/wireless/why-haitis-cellphone-networks-failed/2 (accessed January 2, 2012).

72. Xiaoqiao Meng et. al., *Analysis of the Reliability of a Nationwide Short Message Service* (Paper prepared for IEEE, INFOCOM 2007, 26th IEEE International Conference on Computer Communications, May 6-12, 2007), http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.76.2465&rep=rep1&type=pdf (accessed January 2, 2012).

73. As an example, in Title 10 status, NORTHCOM is funded for some interagency coordination, like the National Level Exercise (NLE) program conducted with DHS. National Guard State HQs fund interagency coordination through their Domestic Operations staffs. Specific unit activities must be funded from operational accounts as training or reimbursed for actual responses. U.S. Department of Defense, *Quadrennial Defense Review*, (Washington, DC: U.S. Department of Defense, February 1, 2010), xiv, http://www.defense.gov/qdr/images/QDR_as_of_12Feb10_1000.pdf (accessed January 2, 2012).

74. John Stiver and George Becker, "Homeland Defense, Homeland Security and Civil Support Strategic Operations Information Sharing: Operating Concept and Implementation Framework" (March 15, 2010), 5, https://www.intelink.gov/inteldocs/action.php?kt_path_info=ktcore.actions.document.view&fDocumentId=237255, (accessed January 2, 2012, Intelink account and password required).

75. Defense Science Board Task Force on Achieving Interoperability in a Net-Centric Environment, Office of the Under Secretary of Defense for Acquisition, Technology and Logistics, "Creating an Assured Joint DOD and Interagency Interoperable Net-Centric Enterprise," (Washington, DC: U.S. Department of Defense, March 2009), http://www.acq.osd.mil/dsb/reports/ADA498577.pdf (accessed January 2, 2012).

76. The term "local" encompasses county, province, or parish level governments as well as those of cities and towns. This is significant, because, in some states, the authority to request assistance rests with county officials rather than officials of individual communities.

77. National Fire Protection Association, "NFPA 1600: Standard on Disaster/Emergency Management and Business Continuity Programs," Appendix A.

78. Nelson, Sigal, and Zambrano, *Media, Information Systems and Communities: Lessons from Haiti*, 24.

79. Gmail™ is a Google® service and Hotmail® is a Microsoft® service. Both provide free web-based email accounts to users.

80. All Partner Access Network was formerly known as the Asia-Pacific Area Network. *All Partner Access Network About Us Page*, https://community.apan.org/p/about.aspx (accessed January 2, 2012).

81. *HarmonieWEB Partner Organizations Page*, http://www.harmonieweb.org/PartnerOrganizations/Pages/default.aspx (accessed May 7, 2011).

82. *Homeland Security Information Network Page*, http://www.dhs.gov/files/programs/gc_1156888108137.shtm (accessed January 2, 2012).

83. Alabama, Florida, Louisiana, Oregon and Virginia have State Information-Sharing Capabilities. *Virtual USA Page*, http://www.firstresponder.gov/Pages/VirtualUSA.aspx (accessed January 2, 2012).

84. *National Guard Common Operational Picture Page*, https://www.intelink.gov/wiki/National_Guard_Common_Operational_Picture (accessed January 2, 2012, Intelink account and password required); quoting content from the *National Guard Bureau Joint Intelligence Directorate (J2) GIS Handbook*.

85. Virtual USA "focus[es] on cross-jurisdictional information sharing and collaboration among the homeland security and emergency management community." *Virtual USA Page*.

86. *United States Northern Command Situational Awareness Geospatial Enterprise (SAGE) Page*, https://sageearth.northcom.mil (accessed January 2, 2012).

87. *Integrated Common Analytical Viewer (iCAV) Page*, http://www.dhs.gov/files/programs/gc_1217445858859.shtm (accessed January 2, 2012).

88. *Verizon Wireless Network Facts: Network Reliability*, http://aboutus.vzw.com/bestnetwork/network_facts.html (accessed January 2, 2012).

89. Xiaoqiao Meng et. al., *Analysis of the Reliability of a Nationwide Short Message Service*.

90. According to COL Greg Hapgood, Public Affairs Officer for the Iowa National Guard, equality among news organizations is very important. Care must be taken to ensure all organizations are offered the same opportunities to utilize social media content. COL Greg Hapgood interview.

91. "Hashtags are a community-driven convention for adding additional context and metadata to Twitter messages (tweets). They are contained in the body of the message and are created by prefixing a key word with a hash symbol: #hashtag. Hashtags were developed as a means to create 'groupings' on Twitter, without having to change the basic service. Using the correct key word is important so the message can be accessed by the appropriate followers." *CampCrisisNZ volunteer FAQ*, http://wiki.crisiscommons.org/wiki/CrisisCampNZ_volunteer_FAQ (accessed January 2, 2012). Additional information available from *Twitter Help Center: What are Hashtags?* ("#" Symbols), http://support.twitter.com/entries/49309-what-are-hashtags-symbols (accessed January 2, 2012).

92. *Twitter Help Center: About Verified Accounts*, http://support.twitter.com/groups/31-twitter-basics/topics/111-features/articles/119135-about-verified-accounts (accessed January 2, 2012).

93. *Swiftriver Page*, http://ushahidi.com/products/swiftriver-platform (accessed January 2, 2012).

94. Matthew Ingram, "Swift River: Trying to Filter the Social Web Firehose," *Gigaom*, July 26, 2010, http://gigaom.com/2010/07/26/swift-river-trying-to-filter-the-social-web-firehose/ (accessed January 2, 2012).

Coalition Mission Command: Balancing Information Security and Sharing Requirements

1. Barack H. Obama, *National Security Strategy* (Washington, DC: The White House, May 2010): 41.
2. Robert M. Gates, *National Defense Strategy* (Washington, DC: Department of Defense, June 2008): 8.
3. Ibid., 21.
4. U.S. Department of the Army, "Enhancing International Security Assistance Force Preparation," *Stand-To!*, May 14, 2010, http://www.army.mil/standto/archive/2010/05/14/ (accessed October 27, 2010).
5. U.S. Joint Chiefs of Staff, *Joint Intelligence*, Joint Publication 2-0 (Washington, DC: U.S. Joint Staff, June 22, 2007): 110.
6. U.S. Government, *Coalition Management*, Strategic Plans and Policy Directorate Manual J-5M 2350.01, July 5. 2006, unclassified excerpt of the *National Strategic Plan for the War on Terrorism*, Annex G, 4 March 2005. A-D-1. http://jcs.dtic.mil/j5/coalition_management.pdf (accessed October 27, 2010).
7. George W. Bush, *National Strategy for Information Sharing* (Washington, DC: The White House, October 2007): 1.
8. Ibid., 4.
9. Ibid., 25.
10. Clay Wilson, *Network Centric Warfare: Background and Oversight Issues for Congress*, Congressional Research Service (Washington DC: The Library of Congress, June 2, 2004): 26, http://fpc.state.gov/documents/organization/33858.pdf (accessed November 3, 2010.)
11. John M. McConnell, *Information Sharing Strategy* (Washington DC: U.S. Intelligence Community, February 22, 2008): 8.
12. Ibid., 15.
13. Lochithea, "Baconian Reference Book," 2009, linked from *The Francis Bacon Research Trust Home Page*, http://www.fbrt.org.uk/pages/essays/baconian_reference_book_archive.pdf (accessed January 9, 2012), 89.
14. Robert M. Gates, "Letter to Senator Carl Levin," U.S. Secretary of Defense. August 16, 2010, http://www.fas.org/sgp/othergov/dod/gates-wikileaks.pdf (accessed October 27, 2010).
15. Theresa A. Pardo and G. Brian Burke, *Government Worth Having: A Briefing on Interoperability for Government Leaders* (Center for Technology in Government:

University at Albany, State University of New York, October 21, 2008), 8, http://www.ctg.albany.edu/publications/reports/government_worth_having/government_worth_having.pdf. (accessed October 27, 2010).

16. U.S. Joint Chiefs of Staff, *Joint Communications System*, Joint Publication 6-0 (Washington DC: U.S. Department of the Defense, June 10, 2010): III-8.

17. U.S. Joint Chiefs of Staff, *International Military Agreements for Rationalization, Standardization, and Interoperability Between The United States, Its Allies, And Other Friendly Nations*, CJCSI 2700.01C (Washington, DC: U.S. Department of the Defense, February 8, 2008), A-1.

18. John Aclin, "Intelligence as a Tool of Strategy," in *U.S. Army War College Guide to National Security Issues*, 4th edition, Volume 1, "Theory of War and Strategy," J. Boone Bartholomees (Carlisle Barracks PA: Strategic Studies Institute U.S. Army War College, July 2010): 274.

19. United States Department of Defense, "Quadrennial Defense Review Report" February 2010, http://www.defense.gov/qdr/images/QDR_as_of_12Feb10_1000.pdf (accessed January 6, 2011), 90.

20. Brigadier General Brian J. Donahue, *Afghan Mission Network*, U.S. Central Command presentation at Landwarnet 2010, August 3, 2010, http://www.afcea.org/events/landwarnet/10/videos/track1/LWN2010%20Track%201%20Session%203.wmv (accessed October 27, 2010).

21. U.S. Joint Chiefs of Staff. *International Agreements*, CJCSI 2300.01d (Washington DC: U.S. Department of Defense, October 5, 2007), C-1. These agreements may be regionally specific or focused on individual conflicts.

22. U.S. Joint Chiefs of Staff, *Information Operations*, Joint Publication 3-13 (Washington DC: U.S. Department of the Defense, February 13, 2006), VI-2.

23. Henry S. Kenyon, "Information Sharing Crucial to Asian Operations," *Signal Online Magazine*, October 2008, http://www.afcea.org/signal/articles/anmviewer.asp?a=1715&print=yes, (accessed October 27, 2010).

24. Barry Rosenberg. "Can you hear me now? How To Stay Connected In Afghanistan. WIN-T Project Manager Faced Political and Technical Problems in Theater," *Defense Systems*, October 12, 2010, http://defensesystems.com/Articles/2010/10/15/Lessons-Learned-Warfighter-Communications-in-Afghanistan.aspx? Page=1 (accessed October 27, 2010).

25. Lieutenant Commander Mark A. Nicholson, *Piecing Together the Network-Centric Puzzle: Using Operational Functions to Analyze Potential Coalition Partners*, Joint Military Operations Department (Newport, RI: Naval War College February 15, 2005), http://www.dtic.mil/cgi-bin/GetTRDoc?Location=U2&doc=GetTRDoc.pdf&AD= ADA464306, (accessed November 3, 2010), 3.

26. Jeff Zeleny and Helene Cooper, "Obama Says Plot Could Have Been Disrupted," *New York Times*, January 5, 2010, http://www.nytimes.com/2010/01/06/us/politics/ 06obama.html (accessed October 27, 2010).
27. Derek S. Reveron, "Old Allies, New Friends: Intelligence-Sharing in the War on Terror," *Orbis*, Summer 2006, 3.
28. U.S. Department of Defense, *DoD Information Sharing Implementation Plan* (Washington DC: U.S. Department of Defense, April 2009): 19.
29. Ibid., 18.
30. Hiroyuki Tanaka, Rocco Bellanova, Susan Ginsburg, and Paul De Hert, *Transatlantic Information Sharing: At a Crossroads, Migration Policy Institute*, (January 2010), 4, http://www.migrationpolicy.org/pubs/infosharing-Jan2010.pdf, (accessed October 27, 2010).
31. U.S. Department of Defense, *International Agreements*, DoD Directive 5530.3 (Washington, DC: U.S. Department of Defense, February 18, 1991), 14-15.
32. U.S. Joint Chiefs of Staff, *Military Telecommunications Agreements and Arrangements between the United States and Regional Defense Organizations or Friendly Foreign Nations*, CJCSI 6740.01B (Washington, DC: U.S. Department of Defense, March 28, 2008), A-3.
33. Donahue, *Afghan Mission Network*.
34. Vice Admiral Arthur K. Cebrowski, USN, and John J. Garstka, "Network Centric Warfare: Its Origin and Future," *Proceedings* 124:1 (The Naval Institute, Annapolis, MD, January 1998): 28-35.
35. Dag Wilhelmsen, "Afghanistan Mission Network (AMN) in Operational Environment.," briefing slides, Koblenz, Germany, NATO CIS Services Agency, September 2, 2010, http://www.afcea.de/fileadmin/downloads/Fachtagung/Koblenz_2010/6%20Wilhelmsen%20-%20(NU)%20NCSA%20TD%20Presentation%20to%20AFCEA%20Koblenz%20020910%20final.pdf, (accessed December 2, 2010), 10.
36. Donahue, *Afghan Mission Network*.
37. Ibid.
38. General Keith Alexander, Cyberspace Operations Testimony, House Armed Services Committee, Washington, D.C., September 23, 2010, http://www.stratcom.mil/speeches/52/House_Armed_Services_Committee_Cyberspace_Operations_Testimony (accessed December 2, 2010).
39. U.S. Department of Defense, *Joint Operation Planning*, Joint Publication 5-0 (Washington, DC: U.S. Chairmen of the Joint Chiefs of Staff, December 26, 2006), IV-35.
40. Brigadier General Susan Lawrence, as quoted in "Information Sharing Challenges on a Multinational Scale" MITRE, September 2008, http://www.mitre.org/

news/digest/defense_intelligence/09_08/multops.html (accessed December 8, 2010).

41. Harrison Donnelly, "Fielding Networked Battle Command Solutions - Q&A: Brigadier General N. Lee S. Price," *Military Information Technology*, October 2010, http://www.kmimediagroup.com/files/MIT_14-9_final.pdf (accessed December 2, 2010).

42. Ibid.

43. Barack H. Obama, *National Security Strategy*, 41.


U.S. ARMY WAR COLLEGE
Prudens
Futuri
Carlisle Barracks, PA